

AD-A141 492

(12)

SYSTEM SAFETY IN AIRCRAFT ACQUISITION

January 1984

F. Ronald Frola  
C. O. Miller

SELECTED  
MAY 31 1984  
A

DTIC FILE COPY

Prepared pursuant to Department of Defense Contract No. MDA903-81-C-0166 (Task ML214). Views or conclusions contained in this document should not be interpreted as representing official opinion or policy of the Department of Defense. Except for use for Government purposes, permission to quote from or reproduce portions of this document must be obtained from the Logistics Management Institute.

LOGISTICS MANAGEMENT INSTITUTE  
4701 Sangamore Road  
P.O. Box 9489  
Washington, D.C. 20016

84 04 30 075

## PREFACE

Department of Defense (DoD) Instruction 5000.36 establishes basic policy for system safety engineering and management in the DoD. It directs the Assistant Secretary of Defense (Manpower, Reserve Affairs and Logistics) to monitor the application of system safety programs in the DoD acquisition process. This is a significant responsibility, in light of the fact that aviation mishaps and safety-driven modification programs together cost over \$1 billion annually and entails the loss of over 200 lives and 200 aircraft. The Logistics Management Institute was asked to undertake a review of system safety in aircraft acquisition programs for the purpose of identifying management initiatives to strengthen the effectiveness of such efforts; that is, toward the reduction of design-related mishaps and the need for costly modifications and retrofits to correct safety deficiencies.

The study began with a review of the safety engineering and management policies and procedures of the Office of the Secretary of Defense (OSD) and the three Military Departments. In order to understand the implementation of system safety programs, detailed discussions ensued at the military safety centers and at system development commands. Selected highly visible, modern aircraft programs were reviewed with Government and contractor personnel. These personnel included program management as well as safety specialists. Meetings were attended of the Joint Services Safety Conference, a Navy system safety symposium, program-specific system safety groups, industry groups, and the System Safety Society. Thus, a broad-based overview of the current state of system safety within DoD was obtained.

A variety of recommendations are made, many of which are for OSD. However, the Military Departments implement the programs, and that is where much of our attention was focused. Thus, we also offer recommendations to the Military Departments.



Distribution For NTIS CMA&I DTIC TIS Unpublished Identification	
By Distribution/ Availability Codes Agent and/or Special	
List A1	[ ] [ ] [ ]

## ACKNOWLEDGMENTS

We wish to thank the many individuals in the Military Departments who were so generous with their time and information during the course of this study -- these include the members of the Joint Services Safety Conference/ System Safety Panel and the representatives from the safety centers, material development commands and system program offices.

We also are indebted to Mr. Fred Eliot, Chairman of the Electronic Industries Association's System Safety Engineering Committee, for inviting us to attend and participate in the meetings of his committee. As a result, much useful information and insights were obtained.

Finally, we wish to thank our colleague at the Logistics Management Institute, Mr. Donald W. Srull, for his many helpful comments and suggestions and for his assistance in establishing the initial scope and direction of the project.



## Executive Summary

### SYSTEM SAFETY IN AIRCRAFT ACQUISITION

The cost of military aviation mishaps and safety modification and retrofit programs exceeds \$1 billion and entails the loss of over 200 lives and 200 aircraft annually. Better implementation of the Department of Defense's (DoD's) system safety policies, plus some refinements in those policies, can reduce the losses.

System safety is a discipline which addresses all aspects of safety, having its greatest impact when applied during the early design and development stages of a new system. It is the process by which hazards are identified, evaluated, and controlled throughout the life cycle of a system. It is a principal contributor to the understanding and management of risk, with the objective of reducing the cost of mishaps and the need for costly safety-driven modifications after the system is put into operational use. The system safety function is generally embedded in the system engineering and acquisition management activities of organizations and programs, although operational and logistics organizations also have a role. It has evolved as a highly technical discipline employing a variety of safety engineering and management tasks.

Successful system safety programs hold valuable lessons for DoD.

- System safety investments can and do pay off. National Aeronautics and Space Administration's (NASA's) Manned Space Flight Program has had an intensive effort, with heavy involvement of top management, in system safety since the early Apollo fire. Their policy is, simply, "no accidents." It works.
- System safety does not require large investments to be cost-effective. For example, a typical system safety program investment (about \$5 to \$10 million over 10 years for a major program) is well worthwhile if it only results in preventing the loss of a single aircraft

(\$15 million for the AH-64, \$25 million for the F-18, \$200 million for the B-1B).

- An effective system safety program requires top management interest and support. In the acquisition process, the immediacies are schedule, performance, and especially cost. Benefits from investments in system safety show up primarily in the long run and then are observable only indirectly (i.e., as non-accidents and the avoidance of safety modifications). Investments in system safety are easily deferred by those directly involved in an acquisition program. Therefore, it is essential to have interest and support of system safety by "off-line" management at levels high enough to be effective.

Our evaluation of system safety management and practices in DoD reveals substantial opportunities for improvement. The principal findings lie in two areas -- (1) management support and (2) specific improvements in the practice of system safety.

#### Management Support

- The Office of the Secretary of Defense cannot effectively discharge its responsibilities under existing system safety policy (DoD Instruction (DoDI) 5000.36) due to the lack of authorized positions for qualified personnel. There are no experienced system safety professionals in either the Office of the Assistant Secretary of Defense (Manpower, Reserve Affairs and Logistics) (OASD(MRA&L)), or in the Office of the Under Secretary of Defense for Research and Engineering. The responsibility for system safety in OASD(MRA&L) is assigned to the Office of Safety and Occupational Health Policy under the Deputy Assistant Secretary of Defense for Equal Opportunity and Safety Policy. The logical basis for the organizational combination of responsibilities for equal opportunity and safety policy is obscure. Further, the Office of Safety and Occupational Health Policy is (erroneously) perceived as a social program, legislatively mandated by the Occupational Safety and Health Act, rather than a management function directed at the conservation of high value resources. This, in turn, is a symbol of a lack of top-management understanding of and interest in system safety.
- System safety activities in the Air Force enjoy some measure of management support at levels above weapon system program management. The Air Force appears to have reasonably well-funded and well-managed system safety efforts, at least on major aircraft acquisition programs. The Army has made notable progress in system safety and has recently given increased command attention to the subject. Significant opportunities are available for further improvements, all of which require continued support of the top management in the Army Staff and major commands. The Navy needs more support for system safety at the levels of Chief of Naval Operations, Chief of Naval Material, and Commander,

Naval Air Systems Command. Personnel authorizations and funding for system safety are not commensurate with responsibilities assigned under existing Navy directives on system safety.

#### Improved Effectiveness

Important opportunities exist to enhance the effectiveness of system safety practice:

- Improving the man-machine interface; this implies the need for greater integration of system safety and human factors engineering.
- Improving methods for detecting system software hazards, given the heavy reliance of modern aircraft on computers.
- Gaining safety benefits via wider application of new and existing technology, such as advanced flight data recorders, ground proximity warning systems, and collision avoidance systems.
- Writing better contracts with respect to system safety, such as including system safety tasks in the work breakdown structure and including safety in award fee criteria.
- More effectively recruiting, training, and retaining system safety personnel.

To strengthen system safety in DoD, we recommend that:

- The Deputy Secretary of Defense reaffirm his support for strengthened system safety efforts by directing the Military Departments to review and report on the status of their system safety efforts, including their responses to the recommendations of this report.
- The Deputy Secretary of Defense direct revisions to several policy directives: DoD Directive (DoDD) 1000.3 ("Safety and Occupational Health Policy for the Department of Defense"); DoDI 5000.2 ("Major Systems Acquisition Procedures"); DoDI 5000.36 ("System Safety Engineering and Management"); and DoDI 6055.7 ("Mishap Investigation, Reporting and Record-keeping").
- The Assistant Secretary of Defense (Manpower, Reserve Affairs and Logistics) (ASD(MRA&L)) increase the visibility of system safety in the Defense Systems Acquisition Review Council process and in the annual Management-by-Objectives Review of Safety and Occupational Health.
- The ASD(MRA&L) establish a system safety specialist position in the OASD(MRA&L) Office of Safety and Occupational Health Policy.
- The ASD(MRA&L) consider establishing the safety office in OASD(MRA&L) at a higher organizational level, either reporting

directly to the ASD or to the Principal Deputy Assistant Secretary of Defense (MRA&L). (If such a move is organizationally impractical, then we would recommend the office remain where it is, since there is no obvious best place for the activity under the existing DASDs in OASD(MRA&L).)

- The Under Secretary of Defense for Research and Engineering establish a system safety specialist position in the Office of the Director, Defense Test and Evaluation or in an appropriate office under the newly created ASD for Development and Support.

In addition, the Military Departments need to take a variety of actions in the areas of management support, policy, organization, staffing and funding, contracting practices, advanced technology, man-machine interface, and system software.

## TABLE OF CONTENTS

	<u>Page</u>
PREFACE . . . . .	ii
ACKNOWLEDGMENTS . . . . .	iv
EXECUTIVE SUMMARY . . . . .	v
 <u>CHAPTER</u>	
1. THE NEED FOR SYSTEM SAFETY . . . . .	1- 1
What is System Safety? . . . . .	1- 1
The High Cost of Mishaps and Safety Modifications . . . . .	1- 2
Does System Safety Pay Off? . . . . .	1- 4
2. OFFICE OF THE SECRETARY OF DEFENSE . . . . .	2- 1
Policies and Management Support . . . . .	2- 2
Organization and Staffing . . . . .	2- 4
Practices . . . . .	2- 9
Summary . . . . .	2-11
3. U.S. ARMY . . . . .	3- 1
Policies and Management Support . . . . .	3- 1
Organization and Staffing . . . . .	3- 5
Practices . . . . .	3- 6
Summary . . . . .	3- 7
4. U.S. NAVY . . . . .	4- 1
Policies and Management Support . . . . .	4- 1
Organization and Staffing . . . . .	4- 6
Practices . . . . .	4-11
Summary . . . . .	4-14
5. U.S. AIR FORCE . . . . .	5- 1
Policies and Management Support . . . . .	5- 1
Organization and Staffing . . . . .	5- 7
Practices . . . . .	5- 9
Summary . . . . .	5-10

## TABLE OF CONTENTS (CONTINUED)

<u>CHAPTER</u>	<u>Page</u>
6. JOINT SERVICES ACTIVITIES . . . . .	6- 1
The Relationship Between JSSC and SOHP . . . . .	6- 1
Some Similarities in the Departments' Approaches to System Safety . . . . .	6- 2
Some Differences in the Departments' Approaches to System Safety . . . . .	6- 6
Allocation of Personnel, Classification, and Training . . .	6- 7
Summary . . . . .	6-11
7. SPECIAL ISSUES . . . . .	7- 1
Contract Incentives . . . . .	7- 1
Life Cycle Safety Benefits from New Technology . . . . .	7- 4
Human Factors and Safety . . . . .	7- 8
Software System Safety . . . . .	7-12
Safety Information Exchange in a Litigious Society . . . .	7-15
8. RECOMMENDATIONS . . . . .	8- 1
Office of the Secretary of Defense . . . . .	8- 1
U.S. Army . . . . .	8- 6
U.S. Navy . . . . .	8- 7
U.S. Air Force . . . . .	8-10
Joint Services Safety Conference/System Safety Panel . . .	8-10
<u>APPENDIX</u>	
A. GENERAL DUTIES AND RESPONSIBILITIES FOR SYSTEM SAFETY SPECIALIST IN OASD(MRA&L)	
B. GENERAL DUTIES AND RESPONSIBILITIES FOR SYSTEM SAFETY SPECIALIST IN OUSDRE/TEST AND EVALUATION	
C. DEPARTMENT OF DEFENSE INSTRUCTION 5000.36 "SYSTEM SAFETY ENGINEERING AND MANAGEMENT"	
D. REFERENCES	
E. GLOSSARY OF TERMS	

## 1. THE NEED FOR SYSTEM SAFETY

### WHAT IS SYSTEM SAFETY?

System safety is a discipline which addresses all aspects of safety, having its greatest impact when applied during the early design and development stages of a new system. Its basic orientation is to the total "system," and includes anything that could cause or prevent accidents (e.g., hardware, software, people, environment). Particular care is given to subsystem interfaces, since that is where accidents most often originate.

System safety is the process by which hazards are identified, evaluated, and controlled throughout the life cycle of a system. Thus, it is a principal contributor to the understanding and management of risk, with the objective of reducing the cost of mishaps and the need for costly safety-driven modifications after the system is put into operational use. The emphasis is clearly at the design stage. Accordingly, the system safety function is generally embedded in the system engineering and acquisition management activities of organizations and programs, although operational and logistics organizations also have a role.

System safety has evolved as a highly technical discipline employing a variety of safety engineering and management tasks. These tasks include the preparation of accident prevention plans, a variety of hazard analyses during design, development and test, surveys, and investigations. Numerous non-engineering system safety tasks (e.g., identification of requirements, accident/incident investigation, feedback of lessons learned, etc.) are also necessary for an effective program. Thus, operations and management skills integrated with engineering talents are the principal components of system

safety. Other fields such as reliability and human factors should also play a major role.

In relation to other "safeties" (e.g., operational, fire, nuclear, explosive, and industrial safety), system safety is an integrating function. It ensures that all applicable safeties are introduced into programs as soon as appropriate, which usually means very early in the life cycle, and continued through cessation of operations. System safety is like project management in its relation to other safeties. It has its own body of knowledge and tasks and, at the same time, plays a safety coordinating role on behalf of the program.

#### THE HIGH COST OF MISHAPS AND SAFETY MODIFICATIONS

As emphasized in a September 1981 memorandum to the Secretaries of the Military Departments from the Deputy Secretary of Defense the costs associated with aircraft accidents and safety modifications are a major problem [3]. The toll in 1982 was about \$1 billion, including about \$200 million for modifications to correct safety deficiencies. Average annual losses over the past 5 years were about 210 aircraft and a like number of fatalities.

In addition to the loss of life and the dollar value of aircraft, there is the associated loss of combat capability. The Air Force loss of 78 aircraft last year equates to the size of one Tactical Fighter Wing (in a force whose total size consists of 36 Tactical Fighter Wings).

The high cost of modern aircraft makes the current accident rate -- which is good relative to historical rates -- a matter for continuing attention. For example, some representative loss values (cumulative average flyaway costs) for current aircraft are:

- AH-64: \$15.0 million
- F-14: 15.8 million

- F-15: 13.5 million
- F-16: 8.4 million
- F-18: 24.6 million.

Viewed slightly differently, the Air Force losses for just five aircraft models (F-15, F-16, F-4, A-10, F-111) in the past four years have been about \$1.1 billion. The F-14 accidents, again with a relatively good accident rate, have cost over \$750 million in ten years. Army aircraft, which are generally of much lower cost, accounted for \$57 million last year.

The annual cost of aviation accidents to the Department of Defense (DoD) significantly exceeds all other types of DoD military and civilian accidental losses combined, on the order of two-thirds more, even when Federal employee compensation payments for injuries are included (but not including claims under the Federal Tort Claims Act).

It is difficult to identify precisely the cost of safety modifications. As will be further explained in Chapter 6, these data are not readily available due to inadequacies in modification program accounting methods and records. Nevertheless, using available data, it is conservatively estimated that at least \$110 million was spent on 66 safety changes for the F-14 from 1973 to 1982. That \$110 million included engineering costs, kit costs, installation expenses, and publication changes. For the F-15, only the engineering change proposal costs were readily available. Those amounted to approximately \$40 million for 35 safety modifications. Data for both aircraft models pertained only to the airframe and did not include engine modification costs.

Despite the difficulty in obtaining accurate safety modification cost data, safety modifications appear to add at least 15-20 percent to the reported costs of accidents. They, like the accidents themselves, represent quite a cost-saving target for system safety.

### DOES SYSTEM SAFETY PAY OFF?

A specific assessment of system safety payoff is difficult at best. One can hardly "measure" something that does not happen such as an accident that has been prevented. It is like trying to measure how much illness has been avoided by proper nutrition.

Approaches other than absolute measurement can be significant as long as a reasonableness test is applied. For example, data concerning material failure accidents (the category most often related to system safety) could be compared on a relative basis. Through 1981, the F-4 and F-14 aircraft had somewhat similar missions in the Navy. The F-4 did not have a formal system safety program, but the F-14 airframe did. Cumulative material failure accidents for the F-4 occurred at a rate of 9.52/100,000 hours. The comparable F-14 rate was 5.77/100,000 hours. There were even greater differences between the two aircraft during initial fleet operations. These data do not "prove" the merit of a system safety program, however. Other factors such as differences in the state-of-the-art applied in each program, different operational environments, design environments, and different contractors probably contributed to the difference between the F-4 and F-14 accident rates.

Another way of assessing the payoff of system safety is to examine case histories. Success (or failure) stories have never been logged formally; however, examples abound where system safety personnel identified hazards which were corrected before accidents occurred and well before the problem would have been identified otherwise. The following examples are illustrative:

- During the design of the F-18, an increase in fire hazard was avoided when a system safety engineer convinced program decisionmakers that a proposed increase in allowable bleed air duct temperature was dangerous. It was also pointed out that a similar hazard could be avoided by ensuring that the bleed air shutoff valve closed when power was removed. A change was made accordingly.

- During a modification to the B-52, a system safety engineer noted that if the front lugs of the Air-Launched Cruise Missile attachment retracted but the rear ones did not, parts of the pylon would tear from the wing and, together with the missile, would inflict severe structural damage to the wing and possibly the horizontal stabilizer. The system was redesigned.
- In a similar case, the CH-47D originally had a single-point hook for load lifting. To improve load retention, a three-point attachment was designed. The system safety engineer discovered that if one hook were to hang up with the others open, it was quite probable that the aircraft could not be controlled, and a good chance existed that cables might actually contact rotor blades. The redesign assured that all hooks opened or none of them did.
- A safety engineer found in the PAVE LOW helicopter system that loss of voltage in a radar circuit would cause a command to the aircraft to fly at zero altitude with no warning to the pilot. He also checked with personnel on the RF-4C and A7D programs, knowing they used the same system. All aircraft were quickly prohibited from flying certain low-level missions until the systems were corrected.

Cases have also been reported where system safety recommendations were not followed and an accident occurred. For example, a project manager decided to eliminate a "roll-over" fuel valve in a helicopter crashworthy fuel system on the grounds of cost savings only to have it reincorporated after an accident demonstrated the need for it. In a similar instance, a change was made to an airplane for value engineering reasons without system safety review, and the changed configuration produced an accident.

One answer to the question of the efficacy of system safety programs can be found from testimonials from those who have "been there." For example, some contractors funded system safety efforts (not necessarily by that name) in aircraft programs as early as the late 1950s. They continue to have respected system safety organizations as part of their company structure. The first several years of the F-14 system safety program were implemented by the contractor, although not funded directly under the contract. At the time, the Navy refused to pay for it, but later did so.

The ballistic missile losses around 1960 gave rise to today's formal system safety programs. No one since then has ever suggested that such programs be rescinded. They are stronger than ever and have expanded well beyond the missile per se.

The National Aeronautics and Space Administration (NASA) has endorsed extensive system safety programs since the 1967 Apollo fire which also triggered major changes to NASA's safety management structure. Today, an extensive system safety program effort is being made on the space shuttle at both the NASA and contractor level. The "save" of the shuttle when the hydrogen fuel leak occurred early this year is reported to have resulted directly from actions taken by Rockwell's system safety personnel.

The most visible DoD aircraft program today, the B-1B Bomber (B-1B) program, provides the most clearcut example of program management backing of system safety observed during this study. Contractor and Air Force safety personnel involvement in program decisions and System Program Office (SPO) support have been obvious. At \$200 million per airplane, the safety investment began with program initiation and has never been questioned.

Costs of system safety programs are quite small in proportion to contract costs. The contractor part of the F-14 system safety program was only about \$5 million for ten years (less than one-third of the cost of an airplane today). A really large program (e.g., B-1B) might have 30-40 Government and contractor people involved at a peak period. Most programs need only one or two system safety personnel in the Government program office and four or five at the peak of the contractor's effort. One person can monitor several sub-system programs simultaneously. Clearly, the saving of just one aircraft by a system safety program pays for that program many times over.

When, then, does a system safety program not pay off? As will become more apparent in subsequent chapters, system safety can be ineffective if top management support is lacking above the level of program management or not plainly visible to all those below and adjacent in the organization, or if insufficient qualified personnel are assigned to the task.

## 2. OFFICE OF THE SECRETARY OF DEFENSE

In May 1976, a "Study of Safety Management" was released by the DoD Management Study Group. The report was critical of the Office of the Secretary of Defense (OSD) in several areas: policy-making, organization, staffing, and planning, programming and budgeting. Within DoD it found, for example:

- There was no specification of safety program objectives in either the Planning, Programming and Budgeting (PPB) or Management by Objectives (MBO) structure.
- There was no formal process of balancing or setting priorities among safety and other programs or among disciplines within the safety programs.
- There was no way to identify expenditures for safety programs in the DoD budget.
- Safety had never been realized as a separate and distinct discipline in the mission of DoD.

It is noted that the 1976 study was motivated principally by criticism of DoD in matters of occupational safety and health for DoD personnel, as distinguished from concern for weapon system safety. Accordingly, the justification for and initial thrust of the resulting increased OSD safety effort, starting in the mid-70s, was in occupational safety and health. This current study, although limited to aviation system safety, has revealed a much improved picture of the management and practice of the various safety fields throughout DoD. Some of the above deficiencies still remain, but to a lesser degree. Much of the improvement is due to the initiatives of the incumbent Director of the Office of Safety and Occupational Health Policy (SOHP), which is particularly significant given his extremely limited resources.

What is needed at the OSD level today is clarification of system safety in the terms expressed in Chapter 1, unequivocal top-level management support

for system safety, improvements in organization and staffing, and, in general, a strengthening of OSD's ability to carry out its responsibilities under existing policies.

#### POLICIES AND MANAGEMENT SUPPORT

The principal document expressing broad DoD safety policy is DoD Directive (DoDD) 1000.3, "Safety and Occupational Health Policy for the Department of Defense" (Mar 29, 1979). For system safety, the key document is DoD Instruction (DoDI) 5000.36, "System Safety Engineering and Management" (Dec 6, 1978). The only deficiency noted in DoDD 1000.3 is that the sole reference to system safety is incomplete. Section D(h) states the Assistant Secretary of Defense (Manpower, Reserve Affairs and Logistics) (ASD(MRA&L)) shall:

In coordination with the USDRE [Under Secretary of Defense for Research and Engineering], assure the application of system safety engineering principles as well as appropriate SOH [Safety and Occupational Health] standards, in the acquisition and life cycle support of DoD weapon systems. . . .

There is no mention of system safety management, only "engineering."

DoDI 5000.36 is generally in keeping with a proper definition and understanding of system safety. It assigns responsibility to ASD(MRA&L) to "monitor the application of system safety in the DoD acquisition process." It applies to all DoD "Components" and directs that all "Heads of DoD Components shall . . . establish system safety programs and apply MIL-STD-882A [Military Standard]. . . ." The directive is implemented through the Offices of the Deputy Assistant Secretary for Equal Opportunity and Safety Policy (EOSP) and its SOHP.

Some vagueness remains in DoDI 5000.36 as to how life-cycle system safety activities will be pursued. The instruction does not identify the organizational elements in Office of the Assistant Secretary of Defense (Manpower,

Reserve Affairs and Logistics) (OASD(MRA&L)) and Office of the Under Secretary of Defense for Research and Engineering (OUSDRE) responsible for system safety; nor does it sufficiently state the responsibilities of ASD(MRA&L) and USDRE. There is no direct assignment of system safety responsibilities to USDRE, but ASD(MRA&L) is required "in coordination with the Undersecretary of Defense for Research and Engineering, [to] establish and support system safety engineering research projects." (Note only research projects.) Further, the responsibilities assigned to ASD(MRA&L) are only very broadly stated: (1) to monitor the application of system safety programs in the DoD acquisition process, (2) to review the "for comment" decision coordinating papers (DCPs) to ensure that safety risks have been addressed, and (3) to coordinate with USDRE in sponsoring research projects.

The perceived inadequacies of the above definition of responsibilities are that (1) there is no indication of how system safety monitoring is to be accomplished, and (2) the review of "for comment" DCPs can result (and does) in a simple statement by the weapon system developer that no significant hazards exist, and there is no provision for OSD to inquire further. Also, OSD is assigned no responsibilities for system safety activities during deployment. Even the Military Departments' role (in DoDI 5000.36) beyond acquisition is related only to change control and disposal of hazardous materials for the system.

It is recognized that DoD directives generally do not delineate organizational duties and responsibilities below the assistant secretary level. However, neither are OSD's responsibilities for system safety specified in writing anywhere else.

A related document, DoDI 5000.2, "Major System Acquisition Procedures" (Mar 8, 1983), states that safety will be included in the Defense Systems

Acquisition Review Council (DSARCs) only on an "as required" basis (paragraph C7 of enclosure 5). (It is interesting to note that reliability and maintainability factors are mandatory items for discussion.) This makes it more difficult to monitor the application of system safety programs since it appears that the Departments may use their discretion as to just what they will present in this regard.

Fortunately, SOHP has not allowed these loopholes to entirely preclude it from monitoring system safety programs for systems in the acquisition process. For example, recently pre-DSARC briefings on system safety matters have been informally arranged. Coordination has been effected with OUSDRE to bring research and safety personnel from the Departments together in a recent conference. Without clearly defined policy guidance and concomitant authority, however, the task of discharging the assigned responsibilities becomes exceedingly difficult.

An encouraging recent development was the inclusion of a reference to system safety in the FY 1984 "Defense Guidance":

Reduction of Accidental Losses. Defense Components shall program actions to reduce serious annual loss of defense resources . . . Specific effort will be directed to . . . strengthen the management of system safety engineering during the design phase of defense systems and facilities to prevent catastrophic accidents and costly safety retrofits. . . .

#### ORGANIZATION AND STAFFING

The 1976 study of OSD safety management observed the importance of the DoD safety office reporting to the highest practicable level. An office so located would project a degree of line authority by virtue of its position in the DoD hierarchy, even though it would really be a staff, advisory function. Visibility, effectiveness in dealing with DoD components and other agencies independent of personalities, and uniformity of policy were all points which favored a safety office reporting at the Deputy Secretary level.

Such an arrangement would have been a major change in the role of the safety office and, more importantly, a major change in the Deputy Secretary's use of his support staff. Such changes were considered then, as they would be now, disadvantages, at least when isolated from other organization questions within DoD.

The 1976 study concluded: "There is no clear cut case for placing the responsibility for safety and health in any particular part of OSD." The same situation exists today; that is, the need to balance the optimum positioning of safety consistent with current DoD organizational structure and methods of operation.

In any event, the OSD safety function has resided within OASD(MRA&L) or its equivalent segment of OSD since the early 1970s. Its heritage was in the personnel safety area; hence its tie to "Manpower." It assumed the broader safety role only after the 1976 study. Indeed, the DoD Management Study Group found it necessary to highlight the importance of understanding the "Safety and Occupational Health" title as it relates to all aspects of safety since then, as now, the scope of "safety" was often misunderstood.

One of the problems today in system safety within OASD(MRA&L) is the perception of that function. The problem begins with the limited description of the safety duties and functions of that office [4]. "Safety and accident prevention" is the only phrase found. It is just one of 33 items of responsibility assigned to the ASD(MRA&L), and includes such others as "postal policy" and "federal-state" relations. The 33 responsibilities are (by the very definition of OASD(MRA&L)) predominantly not associated with weapon system development and not acquisition task oriented.

Also, because OSD's safety function resides within OASD(MRA&L), the inference can be drawn that OSD identifies safety only with the deployment and

operation of systems. Such an inference, however, would not be consistent with the life cycle intent of DoDI 5000.36.

Placing safety in OASD(MRA&L) separates it to a degree from that part of OSD charged with system development and so enables it to think somewhat more independently when safety questions arise during acquisition. Thus, if it is not practicable to have a safety policy office at the Deputy Secretary level, a good alternative is with OASD(MRA&L).

From there, however, the current organizational arrangement leaves something to be desired. The SOHP office is where the first really qualified safety personnel are found. Between that office and the ASD(MRA&L) is the office of EOSP, a unique joining of equal opportunity and safety. The clear (but incorrect) implication is that safety involves only people. One of EOSP's tasks is "to direct special emphasis programs to reduce losses due to mishaps in selected areas [5]." That goes well beyond personnel safety.

Delegation of safety tasks is appropriate, but placing the safety professionals four levels down from the Secretary (or three from the Deputy Secretary) does not project high-level DoD support for safety. Placing SOHP under EOSP reinforces the perception that safety in OSD still means only personnel safety. While that function is important, personnel protection in the workplace is not or should not be DoD's only safety consideration. Rather, conservation of all resources to preserve combat capability should be the objective.

Still another problem is SOHP's incomplete coverage of all the safety fields. It accounts for aviation, explosives, fire, radiation, chemical (partially), ground, occupational, and system safety. It does not cover missile or nuclear weapon safety at all. This point is really academic, however, because of the minimal staffing of the SOHP office.

An even greater shortcoming than anything associated with SOHP is the absence of any identifiable system safety function in OUSDRE. Two potential areas have been involved, but only limited progress has been made.

A memorandum of 24 May 1982 established an individual within OUSDRE as a "focal point for systems [sic] safety research and engineering [and to] facilitate coordination with other elements [of OUSDRE] as required [6]." This resulted in an excellent Joint Aircraft Technology and Safety Review conference at Wright-Patterson Air Force Base earlier this year. The potential safety problems induced by advanced technology were discussed, and the concept of system safety was introduced to the research and development people. It was obvious from this meeting that much more coordination will be needed in the future. This kind of periodic information exchange obviously will not be an adequate substitute for the necessary day-to-day system safety activity needed in OUSDRE.

Another office within OUSDRE has displayed interest in system safety. That is Defense Materiel Specifications and Standards Office (DMSSO), the standards office. It has provided considerable assistance in revising MIL-STD-882A and has expressed a willingness to develop a family of safety standards. However, its basic OSD function is too limited for it to be the OUSDRE safety focal point.

A much more logical location for a system safety function in OUSDRE is under the Director of Defense Test and Evaluation. This office is chartered to be involved with test and evaluation aspects of individual weapon systems, including the review of test and evaluation master plans (TEMPS) and test results. Thus, they are directly involved with program details. For example, they already track reliability and maintainability considerations during acquisition in preparation for test activities [7]. System Safety needs to be

reviewed prior to and during flight test, as flight-test center personnel pointed out during this study. System safety has had strong ties with flight test at many aerospace companies, and some system safety groups report there rather than to functional engineering departments.

One final matter concerning DoD safety organization involves the DoD Safety and Occupational Health Council. Resulting from the 1976 study, required by DoDD 1000.3 and cited as a "policy" council in DoDI 6055.7, it deals primarily with occupational safety and health (OSH) matters. This council satisfies the safety council requirement in OSH statutes by coordinating OSH efforts among the Departments and providing high-level management visibility to such problems. System safety has been addressed in these meetings only peripherally.

Still, the council illustrates an organizational concept applicable to system safety. Given the limits of system safety integration possible within OSD, a System Safety Review Board (or a group with some such title to distinguish it from the council) could bring group dynamics to bear on improving weapon system safety. If attended by high-level OASD(MRA&L) and OUSDRE personnel, among others, it could lead to significant improvements.

Staffing is closely allied to organization. Within OSD and at least one of the Departments, safety staffing is clearly inadequate. There are only three safety positions (none of which are for system safety specialists) in the SOHP office, hardly enough for a meaningful effort on the occupational safety and health side, let alone on system safety. No one in OUSDRE has a background in system safety, much less an assignment to carry out that function. Large staffs are not endemic to system safety endeavors; however, personnel levels greater than zero are necessary to have the function at all.

DoDI 5000.2 refers to "principal advisors" in OUSDRE for reliability, maintainability, and quality control. System safety should be accorded the same recognition.

#### PRACTICES

Many of OSD's system safety practices have already been discussed. Additional observations are appropriate, however, especially from sources outside OSD.

Many contractors perceived safety activities at the OSD level as either nonexistent or associated only with protection of the Federal work force. Little interest in system safety was seen at the OSD level except for the SOHP Director's participation in system safety professional meetings. ASD(MRA&L)'s role in acquisition was not recognized whatsoever. Combining equal opportunity with safety was viewed as demeaning both areas. The existence of SOHP was usually not known; when it was, the perception was that its interest was not significantly weapon system safety.

The Military Department personnel's perceptions were somewhat more positive, particularly because of the active liaison of the SOHP office with the Joint Services Safety Conferences (JSSC). Only there, and especially among members of the System Safety Panel, were the safety functions and duties of OSD offices known. Even there OASD(MRA&L) was (correctly) not perceived as playing an active role in DSARC, and OASD(MRA&L)'s safety function was viewed as concentrated in areas other than aviation or other weapon systems.

Secretary Weinberger's memo of 7 January 1983 fostered such a perception [8]. Although it mentioned system safety engineering, it was entitled "Occupational Safety and Health"; it spoke first to workplace hazard abatement and health surveillance, and was seen as motivated by a memorandum from the White House sponsored by the Department of Labor on the subject of the occupational health and safety of the Federal workforce.

The annual MBO review of safety and occupational health programs provides perhaps the only, and certainly the best, opportunity for the ASD(MRA&L) to make a formal assessment of system safety programs in the Military Departments. These reviews are not utilized for this purpose, however, and are devoted instead to aspects of safety other than system safety. Consequently, the impression is that OSD's safety priorities continue to be in the non-weapon-system area.

DoDI 6055.7, which is the instruction governing the MBO reporting, is mainly a mishap reporting procedure. It is entitled, "Mishap Investigation, Reporting and Recordkeeping" and contains great detail on mishap classification and accounting practices. There is nothing in DoDI 6055.7 that would preclude system safety from being included. In fact, provision is made for "analysis of principal problem areas, causal factors, and corrective action . . .", and for "special interest items prescribed separately."

Attitudes projected to the Services in the MBO meetings and compliance requirements can and do influence thinking at the Service level. The results suggest that the Services believe OSD is far more interested in private motor vehicle accidents, industrial injuries and worker compensations, fires, etc., than they are in major weapon system safety. Whether true or not, that image is being projected and has the net effect of inhibiting (or, at least, failing to promote) effective aviation system safety efforts or any other system safety effort.

The theoretical coordination between OASD(MRA&L) and OUSDRE through SOHP has recently begun to function to some degree in practice. The fact remains that an SOHP office with or without adequate staff is not close enough to day-to-day OUSDRE activities (in acquisition or research and development) to be as effective as it needs to be. As a case in point,

consider the \$227 million Software Technology for Adaptable, Reliable Systems (STARS) initiative proposed earlier this year. Despite considerable system safety concern about software-induced hazards, the term "safety" never appeared in the STARS development program [9]. Similarly, flight data recorders, maintenance recorders, performance monitors, V-G recorders, etc., were developed independently when system safety thinking would have suggested their development in a much more coordinated fashion.

In any case, one cannot really fault SOHP. That office has made remarkable progress despite the lack of appropriate staff and the organizational problems noted earlier. Furthermore, SOHP visibility within and above OASD(MRA&L) appears to be at least reasonable. Through the personal encouragement of the SOHP Director, JSSC, including its system safety panel, remains an excellent link between OSD and the Services' system safety efforts today.

#### SUMMARY

OSD safety management has certainly advanced since 1976. Some policy matters need to be corrected, but they are relatively minor. System safety improvements have been directed in the FY 1984 Defense Guidance. Attempts have been made at OASD(MRA&L) coordination with OUSDRE. The MBO and JSSC meetings provide viable communication between OSD and the Departments.

The main problems seem to be in the implementation of system safety. There are some fundamental organization and staffing problems, coupled with a general misunderstanding of system safety's role vis-a-vis the other safeties.

Organizationally, OASD(MRA&L) has a problem in its EOSP/SOHP arrangement which, because of the nature of the safety business, has a direct bearing on the effectiveness of accident prevention efforts. Also, OUSDRE is not involved with system safety as they most certainly should be.

The SOHP office is neither reasonably nor effectively able to discharge its responsibilities. It is helping where it can, but it has too few qualified personnel. It cannot be effective in the DSARC process under existing organizational and personnel constraints.

Finally, there has been no projection of high-level interest in system safety since the Deputy Secretary of Defense's memorandum of September 1981. This is particularly significant since Mr. Thayer has replaced Mr. Carlucci and because policies are identified with individuals as well as with paper. OSD's position on system safety, indeed on all safeties, needs to be clarified.

### 3. U.S. ARMY

#### POLICIES AND MANAGEMENT SUPPORT

Characteristic of all the Services that function as developers of major weapon systems, the Army's regulations identify its policies, functions, and responsibilities regarding system safety. They pertain to systems acquisition and to safety as such. Typically, the top-level safety document is amplified by a system safety regulation which, in turn, is supplemented by subordinate commands as necessary. The resultant hierarchy of regulations, associated explanatory manuals, and occasional command messages describes Army policies and management support for system safety.

Army Regulation (AR) 1000-1, "Basic Policies for Systems Acquisition," sets safety policy at the acquisition stage. It refers to system safety under a "Safety and Health" section and requires "maximum efforts . . . to coordinate matters of mutual interest among . . . safety . . . health . . . [and] human factors." It directs materiel developers to ensure that "adequate funds are programmed for . . . system safety planning and assessment."

"The Army Safety Program," AR 385-10 is the oldest top safety program document. It implements DoDD 1000.3 and refers by number to AR 385-16, "System Safety Engineering and Management." It also lists various hazard analysis techniques. Otherwise, like DoDD 1000.3, AR 385-10 conveys the impression of emphasizing personnel safety rather than weapon system safety.

AR 385-16 provides detailed requirements implementing DoDI 5000.36 and MIL-STD-882A (the military system safety standard). System safety objectives are stated particularly well and include life-cycle hazard control, concern for new materials/designs, and the need to reduce retrofits. AR 385-16 adds

"health" to the scope of system safety, the only Department regulation to do so at this level.

Under AR 385-16, the Deputy Chief of Staff (DCS) for Personnel, assisted by the Commander, Army Safety Center (ASC), sets system safety policy. Other commanders with specific system safety obligations include DCS for Research, Development and Acquisition; DCS for Operations and Plans; the Chief of Engineers; the Surgeon General; major commands (users, combat developers, materiel developers); Test and Evaluation; and installation commanders.

Good safety engineering and management practices are illustrated by such requirements as a Safety Assessment Report from the materiel developer prior to test and evaluation and a Safety Release procedure prior to test. Types of hazard analyses are added as appendices. The only item missing is reference to the integration of the various activities in life cycle terms. The implication is that coordination is a basic function of each organizational segment; however, with life cycle coordination being such an integral part of the system safety concept, it is best not left up to assumption.

The Department of the Army Materiel Development and Readiness Command (DARCOM) Supplement 1 to AR 385-16 is a textbook for implementing system safety during materiel development. It clearly directs "program/project/product managers" among others to "provide adequate resources for . . . an effective system safety effort." It also calls for "integrating system safety engineering into the total system acquisition program . . . [and] assuring the local safety director is advised of new design concepts . . ." and sets forth other tasks implicit in a good system safety program.

DARCOM has a "System Safety Management and Engineering Action Committee" to provide timely exchange of system safety management and engineering information within the command, advance the state of the art in system safety,

increase professional competency, and establish liaison with other similar groups (such as JSSC and the System Safety Committee of the Electronics Industries Association (G-48)). This is an excellent safety management undertaking.

Other regulations specify functions at the aviation system development level. For example, DARCOM Regulation 10-72 specifies that the Army Aviation Research and Development Command (AVRADCOM) shall "provide for safety engineering in the design of aircraft systems, subsystems, and support equipment for personnel accident reduction, operational safety, safety-of-flight, radiological, and other safety considerations," a broad scope of activity. AVRADCOM Regulation 10-1 provides the charter for the command's system safety office, and orders it to "report unresolved system safety program matters to the Commander." Other duties shown in AVRADCOM Regulation 10-1 constitute a superb checklist of system safety functions for offices of this type.

The Troop Support and Readiness Command (TSARCOM) Supplement 1 to AR 385-16 is a similarly explicit statement of system safety duties and functions. Since TSARCOM is a downstream activity, those include the task of coordinating system safety data transfer as new systems enter TSARCOM's control.

During this study, AVRADCOM and TSARCOM were in the process of being combined into a single Aviation Systems Command, AVSYSCOM, to become effective in April 1984. The system safety requirements are not expected to change.

The Training and Doctrine Command (TRADOC) and the Forces Command (FORSCOM) have also recently supplemented AR 385-16 to extend system safety engineering and management requirements into their safety programs. TRADOC, for example, requires a "safety release" from the Safety Office prior to conduct of test programs. They also identify responsibilities for combat

development activities to include staff safety visits, attendance of safety personnel at meetings to prepare requirements, and review of various requirements documents for safety input.

Only the Operational Test and Evaluation Agency (OTEA) does not seem to have endorsed system safety with a program. On the contrary, comments were made that OTEA tended to believe they should deliberately avoid knowledge of much of what had transpired upstream in the life cycle so that their tests and evaluations could be highly objective. They recognize the requirement to test safely, but not necessarily to test for safety. They do not seem to realize the benefit of their participation in upstream system safety efforts.

Excellent policy and management support for system safety has been in place for Army aircraft acquisition for some time. As recently as 27 June 1983, still another emphatic expression of support came from Deputy Chief of Staff for Personnel (DCSPER). In a message entitled "Enhancement of the Army Safety Program," a basic theme was stated succinctly, "safety accomplishment is not just business as usual." Furthermore, several new initiatives were noted: system safety is to be addressed at Army System Acquisition Review Council (ASARC) through proponentcy of DCSPER; safety subject matter is to become more evident in Army schools; there shall be new and revitalized command involvement in an emphasis on safety and "where appropriate, pull all the pieces of your safety program together."

This top-level commitment to safety typifies the positive attitude toward system safety encountered among Army personnel at all activities visited during this study. It is probably the key factor in the Army's growing adoption of system safety approaches over the past ten to fifteen years.

## ORGANIZATION AND STAFFING

The line or decision authority organization for aviation system safety is from DCSPER to DARCOM to AVRADCOM/TSARCOM to program and functional offices. The safety director at AVRADCOM is at the O-6 (Colonel) level.

Delegation of system safety tasks and duties follows a very modern approach. Both project and functional responsibilities are seen at the program level. Personnel are assigned to programs but also have a functional (technical) home. The functional supervisor has a relatively independent path to higher authorities should he elect to use it. Coordination with other areas has been noted, although inadequate with respect to human factors engineering involvement in system safety efforts.

Staff or advisory input is provided not only by the functional safety offices at the program level but also by the ASC. ASC's origin was in aviation, and it has been a major supporter of system safety in the Army and in the aerospace community as a whole. It was their initiative during the early 1970s which produced the first comprehensive Army Aircraft system safety program (for the UH-60).

System safety at ASC is within the Systems Engineering section of the Systems Management Division. This is generally a very good alignment since the Systems Management Division addresses the prevention side of the safety house. Some earlier tendency was observed for ASC to look only to the engineering side of system safety, not unlike several other activities encountered during this study. However, ASC realizes that OTEA, TRADOC, FORSCOM, and others at the using end of the system safety spectrum are deficient in their support of system safety, and that continuing command emphasis will be necessary to correct these deficiencies.

ASC's role in the acquisition process has been recently clarified as an advisor to DCSPER on designated acquisition programs. In addition to providing an independent voice on system safety, this helps assure that "lessons learned" from previous programs will not be lost on the way to ASARCs.

System safety staffing in the Army aviation area has been generally satisfactory, though spartan in quantity. There were minimal complaints from personnel interviewed and a genuine effort seemed to be present to work effectively within current economic constraints. System safety personnel were most concerned with the likelihood of deteriorating quality since the DARCOM-sponsored graduate training programs for system safety personnel no longer exist. An even more important factor is that civilian personnel position mobility and grade levels within the system safety field are limited, causing qualified people to go elsewhere for career and salary advances. (This subject is treated further in Chapter 6.)

#### PRACTICES

The foregoing observations were based on visits to Headquarters DARCOM, AVRADCOM, and ASC and, also on examination of the UH-60 program and the Army's current major development program, the AH-64, including discussions with contractor personnel. These system safety efforts appear to be adhering to published policies and requirements. On the AH-64 program, the work breakdown structure to the level of system safety tasks ensures control of safety funding and is permitting realistic monitoring of system safety efforts. Personnel seem to be well qualified, and the system safety program seems to be on track.

Other indicators of professional system safety efforts were also seen. An excellent "how-to" manual had been prepared, "System Safety," DARCOM Pamphlet 385-23. It is particularly effective, for example, in describing

system safety's role in the program/project office. Also, DARCOM, with assistance from ASC, is developing a series of system safety design guides, one of which focuses on aviation.

The principal weaknesses observed are: (1) the lack of participation by OTEA in system safety, (2) the lack of system safety involvement in research and development programs (e.g., composite materials, fly-by-wire flight control systems), (3) inadequate involvement of human factors engineering in system safety, (4) insufficient system safety review in modification programs, (5) the need to improve AR 385-10 relative to system safety, and (6) the need for better integration of system safety efforts over the life cycle of weapon systems.

#### SUMMARY

As noted above, there are a number of areas in which the Army can strengthen its system safety efforts. Notwithstanding these shortcomings, the Army has made significant progress in system safety.

Over 20 years ago, the Army began the research that led to its highly successful safety engineering and management effort towards crash survivability coupled with personnel protection in combat. That program demonstrated that hazards could be avoided in designing the aircraft, given the necessary specialized engineering and management attention. Today, the resolve that produced that historic breakthrough in air safety is still present. Moreover, broader-based system safety policies are now in place, providing the basis for further improvements in system safety practices. Specific tasks are identified and controlled during acquisition, at least for the current major aircraft programs. Safety contributes to, but does not restrict, combat readiness.

#### 4. U.S. NAVY

##### POLICIES AND MANAGEMENT SUPPORT

The hierarchy of Navy safety requirements documents provides some insight into the Navy's policies and management support for system safety. They begin at the highest level in the Naval establishment, the Office of the Secretary of the Navy (SECNAV).

SECNAVINST 5100.10E, "Department of the Navy Safety and Occupational Health Policy; Implementation of," was prepared in response to DoDI 1000.3 and related DoD directives. It provides "current policy and assign(s) responsibility for the Department of the Navy accident prevention, safety, and occupational health programs." Paragraph 3h directs application of "System Safety Management and Engineering principles . . . to acquisition programs (and) throughout the life cycle" per DoDI 5000.36. Furthermore, it calls for program planning, including budgeting, to "ensure system safety performance goals . . . are consistent with other program management goals" and requires independent safety assessments prior to the Department of the Navy Systems Acquisition Review Council (DNSARC) reviews at Milestones I, II and III.

SECNAVINST 5100.10E identifies the Assistant Secretary of the Navy (Shipbuilding and Logistics) (ASNS&L) as the "designated safety and occupational health official . . . [who] shall establish, maintain and modify, as appropriate, safety and occupational health programs which implement the requirements of DoD policy issuances to provide protection for both civilian employees and military personnel." It also directs ASNS&L to ensure "action is taken during the acquisition process to include system safety management and engineering principles and assure an independent safety assessment is

performed during DNSARC reviews" (paragraph 6a(5)). Finally, it directs the Chief of Naval Operations (CNO) to "develop and implement a system safety program to support all phases of the system life cycle beginning with the engineering development through the acquisition process, including independent assessment/ review at Milestones I, II and III" (paragraph 6b(18)).

These appear to be reasonable policy statements regarding system safety. It is noted, however, that the references to system safety were only added to the instruction on 14 February 1983. Further, this instruction has traditionally been purely an occupational safety and health document, and even its current version encourages such a perception. The above cited paragraphs plus one more, 6b(15), requiring boilerplate adherence to MIL-STD-882A, are the only references to system safety in the instruction's eight pages. Occupational safety and health matters are treated in great detail, e.g., CNO is directed to ensure "employees . . . shall have access to workplace records" (paragraph 6b(3)(d)), or to "provide for job related medical support such as immunizations" (paragraph 6b(6)).

CNO's safety policy is found in OPNAVINST 5100.8F, "Navy Safety and Occupational Health Program: implementation of," 23 September 1983. This latest modification to a long standing requirement was triggered by the formation of the Office of the CNO Safety and Occupational Health Coordinator, OP-09F. The Navy's Safety objective is stated as "to enhance operational readiness and mission accomplishment by establishing an effective safety . . . program which will, to the . . . maximum extent feasible, reduce occupational injuries, illnesses or deaths and material losses or damage." The phrase "occupational injuries, illnesses or deaths" might appear to be only occupational-safety-oriented, but a broad interpretation would apply to all mishaps injuring or killing DoD personnel.

Paragraph 6a of OPNAVINST 5100.8F assigns OP-09F responsibilities for "Overall Program Coordination." Paragraph 5b(1) describes four "Primary Program Areas": Submarine and Diving, Surface, Shore, and Aviation. In an enclosure, where descriptions and responsibilities of these areas are shown, a fifth area, Explosive Safety, is added. In addition, the enclosure identifies 13 "Specified Support Areas." These are "areas requiring special attention and/or technical expertise." Six have at least an indirect relation to aviation (fire protection, chemical ordnance, hazardous materials, nuclear weapons, non-ionizing radiation, and explosives). System safety is not mentioned.

System safety does appear in the responsibilities assigned to the Chief of Naval Material who shall "insure that the system safety engineering and management principles in (MIL-STD-882A and DoDI 5000.36) are complied with. . . ."

In the responsibility assigned to OP-05 for "Aviation Safety and Occupational Health" (one of the program areas), system safety can, at best, only be inferred. That responsibility is:

All aspects of safety and occupational health in the design, operation, training, maintenance, and support of aircraft, aircraft carriers, and associated equipment.

An earlier CNO instruction which relates to system safety is OPNAVINST 5100.24, "Navy System Safety Engineering and Management." Written in 1979 to implement DoDI 5000.36, it is only about one and one-half pages in length. It speaks to hazard control over the life cycle but the "Action" paragraph speaks only to "commands that contract for, develop in house or buy off-the-shelf systems, equipment test programs [and] facilities."

Another important document with the authority of CNO behind it is "The Naval Aviation Safety Program," OPNAVINST 3750.6N. This document originated

decades ago as an accident investigation handbook and evolved into an accident prevention handbook of sorts. Its title alone says it is a key program document; however, it is oriented heavily towards operational safety and accident report procedures.

Per OPNAVINST 3750.6N, safety program policy emphasizes only one thing: "Safety is an inherent responsibility of command, and the Naval Aviation Safety Program is therefore implemented through the chain of command" (paragraph 101). System safety is only implied, not identified as such, in the "Scope of the Program" (paragraph 104). It is specifically referred to only twice. First, it is mentioned in the program responsibility of the Chief of Naval Material who shall:

Consistent with required military capabilities, ensure that safety aspects are considered, designed, and engineered into all aircraft, aircraft weapons, weapon systems, aviation equipment, materials, supplies and facilities which are acquired, constructed, or provided through the Naval Material Command.

Ensure that the systems (sic) safety engineering and management principles of DoD Military Standard 882A . . . are applied in all activities under Chief of Material cognizance which relate to naval aircraft (paragraph 107C).

Second, system safety is mentioned in the program responsibilities of the Commander, Naval Safety Center (NSC) who shall:

Assist in reviewing and evaluating aviation system safety engineering requirements on new systems and major modifications by participating selectively on boards, at conferences, and in studies and design reviews.

Significantly, references to system safety are absent from other functional descriptions such as those for commanders of operational or support organizations, for Naval Plant Representative Officers, or for the Director, Aviation Safety Programs at the Navy Postgraduate School. (Aviation Safety Officer and Aviation Safety Command courses are included but none for system safety.)

At the level below CNO, NAVMATINST 5100.10 defines "Safety Responsibilities in Designated Project Management Offices within the Naval Material Command." It applies to managers of development, production, and modification programs and requires specific safety objectives, safety responsibilities, and designation of one person to be responsible for executing the safety program (the "Principal for Safety"). This instruction has not been updated since 20 August 1976. It cites a 1969 directive which was issued "to strengthen the attention given to safety matters in the project management area" and a Naval Material Command (NAVMAT) Inspector General (IG) inspection which found that 1969 requirement "not now uniformly implemented among PM's [Program Managers]." System safety was only one of a comprehensive list of safety areas referenced in this instruction.

NAVMAT's basic system safety policy is described in NAVMATINST 5100.6A of 28 February 1980, "System Safety Program; Implementation of." Again, this is a system safety engineering policy. It states onlv that "all acquisition programs shall include a system safety program" (underlining added). Within those bounds, it does follow MIL-STD-882A in depth, including stating the need for funding such an effort. Its provisions call for independent reviews of numerous acquisition documents including Mission Element Needs Statements (MENS), TEMPS, and Request for Proposals (RFPs). It also requires "provision for personnel trained in system safety management principles and system safety engineering techniques."

Aviation system safety policy is further detailed in "Naval Air Systems Command Safety Program," NAVAIRINST 5100.3B, 24 July 1981. This well written instruction is amplified by a valuable appendix, "NAVAIRSYSCOM [Naval Air Systems Command] System Safety Program Management Manual." Citing DoDI 5000.36, SECNAVINST 5100.10E, OPNAVINST 5100.24, and NAVMATINST 5100.6A

as well as referencing MIL-STD-882A, the instruction states the policy of identifying hazards to people or equipment, evaluating risks and benefits against resources, eliminating or controlling risks in NAVAIR products or operations, and ensuring that a formal system safety program is established for each project. Project managers, project coordinators, and all acquisition managers have appropriate system safety tasks assigned. The tasks apply at the beginning of the system life cycle with review of Operational Requirements, Program Objective Memorandums, Requests for Quotations, etc. They continue throughout the life cycle, since the Navy has a single command (NAVAIR) covering both the acquisition and logistics end of system development and deployment of Naval aircraft, unlike the Air Force and the Army.

As will be discussed further in the next section, NAVAIRINST 5100.3B also specifies the system safety responsibilities of the Office of the NAVAIR Director of Safety, test, and other activities throughout the Navy. Significantly absent, however, is any provision for ensuring a cadre of system safety professionals within engineering or any other function. Without sufficient in-house capability, Navy System Safety programs can become little more than ineffective paper exercises by the contractors.

#### ORGANIZATION AND STAFFING

The lines of authority for system safety in the Navy appear simple enough: from SECNAV to CNO to NAVMAT to NAVAIR and to other activities including project/program offices. However, there are complexities both at CNO level and within NAVAIR.

A simple but significant change has occurred at the Office of the SECNAV within the last few months. The title of the top safety person has changed from "Director, Occupational Health and Safety" to "Director, Health, Safety and Environment." Thus, safety has been separated from the purely occupational context.

At CNO, the key office is OP-09F. The person occupying that position is the "principal advisor to the Chief of Naval Operations on safety and health matters." He actually reports to the Vice Chief of Naval Operations (VCNO) as a "CNO Safety and Occupational Health Coordinator," which is established as a "CNO/VCNO Staff Assistant." He is Commander of the NSC functioning in an additional duty capacity. The office also contains a primary-duty captain billet and a secretary.

OP-09F coordinates and advises; it does not direct or implement policy. As stated in OPNAVINST 5100.8F, OP-09F "is responsible for providing compatibility, continuity, and interface between primary program areas [and] provides overall program interface and coordination of the various elements of the Navy program to insure consistency of policy, procedural guidance, and objectives." There are other safety offices within CNO for aviation safety (OP-05F), explosives safety (OP-411F), and environmental protection, occupational safety and health (OP-45). There are none specifically identified with system safety. Up until the formation of OP-09F about a year ago, OP-45 had been thrust into an undesired role of writing system safety instructions and sponsoring NAVAIR's system safety budget submissions. There is no evidence of any organizational integration of the safeties at the CNO level, although recently an informal panel of system safety personnel from all support areas has been meeting under the auspices of OP-09F.

At NAVMAT, the safety office reports to the Deputy Chief of Naval Material (DCNM) for Logistics, which induces the same problem of safety not being identified with acquisition as at OSD(MRA&L). They have specialists in fire protection and occupational safety/health only and have been involved in system safety only peripherally. Specifically, there is no one to discharge the system safety responsibilities assigned in NAVMATINST 5100.6A. The

aircraft system safety acquisition function has really been delegated to NAVAIR without meaningful followup by NAVMAT.

NAVAIR's system safety duties and functions are described in NAVAIRINST 5100.3B. The Safety Directorate, (AIR-09E), reports to the Vice Commander. The Director is "the executive manager within NAVAIR for system safety," with assistance, review, and audit responsibilities. This is essentially a policy-making and monitoring function and is headed by an O-5 level officer (Commander).

Other assignments are given to test and evaluation organizations for hazard evaluation and safety assessment and to other NAVAIR "activities" to establish system safety engineering billets "to develop and implement SSPs (System Safety Programs) in conjunction with projects and tasks assigned to NAVAIR HQ [Headquarters] which relate to technological and product development, acquisition and in-service engineering." This includes Naval Air Rework Facilities (NARFs).

Quite significantly, NAVAIRINST 5100.3B does not identify a functional home for system safety personnel, thus leaving open the question of where qualified project support people are to come from and how they shall receive their technical supervision. NAIR-516C, within the Engineering and Product Integrity Management Division under the Assistant Commander for Systems and Engineering, has been functioning in this capacity and is a logical location. It currently is responsible for dozens of projects and has a severe staffing problem.

NAVAIR uses matrix management, an accepted concept whereby a project manager acquires a team from functional segments within the organization to carry out a particular project. At the completion of the project, the team members return to their home offices. During the project, the functional

office chief provides technical guidance to personnel from his unit and acts as a technical check on the project manager's decisions. Project and functional chiefs usually report to the same official through different chains of command.

NAVAIR's application of matrix management to system safety matters is confusing. Several reasons account for this. First, there is the relationship between the Program Manager - Air (PMA) and the Class Desk Officer. The PMA occupies a higher-level position (especially since he controls the funds) and has safety management responsibilities per NAVMAT/NAVAIR directives. The Class Desk is the project engineering director through whom system safety engineering efforts would funnel. The PMA and the Class Desk are complemented by a "System Manager" at the NARF as the system is deployed. There is no apparent integration of these system safety functions over the life cycle of a system.

The PMA, Class Desk, and System Manager make daily decisions that affect system safety. The PMAs do not have system safety personnel on their staffs. The Class Desk officers often chair system safety group meetings and utilize "principals for safety" on their staffs. These "principals", however, are not necessarily qualified in system safety or linked organizationally to AIR-516C. That "office" is under an engineering integration activity and is the closest thing to a functional center for system safety in NAVAIR. It consists of one man. Thus, there is no functional tie between system safety staff and a technical home base to assure the quality of their input. Further, AIR-516C has neither the people or the power to control the assignment of personnel to support the "principal for safety." It currently obtains help from the Naval Air Engineering Center in Lakehurst, N.J. as a matter of necessity. Plans are underway to perform the system safety support function with outside contractor(s).

Another deficiency in NAVAIR's management of system safety occurs with deployed systems since the NARFs do not yet have system safety programs in place, at least with qualified personnel. Some effort is now underway to correct this situation.

Organization and staffing for system safety at the NSC is also deficient. The System Safety Branch is part of the Maintenance and Material Division, Aviation Directorate, and currently has been proposed as a separate System Safety Division. (NSC's scope has been broadened beyond aviation for several years.) Unfortunately, the unit has only three personnel assigned, only one of whom has had prior system safety experience. In comparison, the ASC has about 10 system safety positions and the Air Force Directorate of Aerospace Safety has about 18.

NSC's system safety personnel and staff members from other sections participate selectively in acquisition-phase activities including attendance at system safety working group meetings. They have been hampered by insufficient travel funds for these efforts (the program offices do not cover such NSC expenses). Within the indicated constraints, NSC has been trying to become more active in system safety and is working on a design safety document and a system safety management guide.

The organizational role of NSC is critically important to system safety. Looking at both system acquisition and fleet operations, it is in the best position to ensure integration of all safety efforts throughout a system's life cycle. To do this, however, it needs to take a broader course than the one portrayed in OPNAVINST 3750.6N.

The coordinator/advisor role at OP-09F needs to be strengthened, at least from the system safety point of view. NSC's expanded role has amplified administrative difficulties at the NSC, particularly with today's limited

budgets. In theory, the CNO/NSC organization as it exists today could work, especially depending on the second-in-command at each office and/or the motivation, background, and interests of the first. Given the physical separation of the NSC (Norfolk) from Washington and current budget realities, continuation of the existing arrangement will be an interesting challenge for the new NSC Commander.

The fact that the NSC Commander wears two hats, the other one being OP-09F, it follows that he has the greatest personal impact in formulating Navy safety policy. To suggest, as some might, that only the CNO (or VCNO) makes policy neglects the real world limits of issues that can occupy his time -- and safety is not likely to be one of them. It is noted that, unless an effective safety coordination program (including system safety) exists at OP-09F, CNO-level safety policy and programs may not adequately reflect (1) SECNAV safety directives, or (2) the needs of the various CNO-level and Naval Material Command safety activities.

#### PRACTICES

The F-18 program is an interesting case in point for some of the matters discussed above. Although the Navy has been fortunate in having several Class Desk officers assigned to this program who were advocates of system safety, only a part-time system safety officer has been assigned in recent years to this costly program. Moreover, the departure early this year of the part-time system safety officer, without a replacement for an appreciable period, illustrates still another staffing problem -- the uncertain and short-term nature of military personnel assignments, which critically affects an activity like system safety with its need for a high degree of continuity.

A few years after the F-18 program began, NAVAIR had to go to the non-aircraft system safety people at Dahlgren Naval Surface Weapon Center to

get technical support. These air-launched missile system safety engineers contributed admirably, but they found almost no signs of "lessons learned" from the A-7, F-4, or F-14 programs being applied in an organized fashion. From the contractor's viewpoint, the system safety program has never seemed to be well defined or actively pursued. Funds presumably allocated to system safety were lumped into sustaining engineering, without a work breakdown structure that protected the use of the funds for accident prevention. The initial contractor effort was a marginal but reasonable four-to-five-man effort, but this decreased to a half-man effort at the very critical time when the aircraft was being introduced into the fleet.

Several other symptoms of the Navy's deficiencies in system safety were also observed. Consider first the JVX program that came over from the Army for management by the Navy. In some undetermined way, the system safety part of the RFP, which had been in the Army's version of the RFP, disappeared before the RFP went out for bid. It was restored by AIR-09E when they learned about it, and an amendment to the original RFP was distributed.

A 16 May 1983 memorandum from CNO, following up SECNAVINST 5100.10E, was entitled "Occupational Safety and Health," not "Safety and Occupational Health" as one would expect. It synthesized the SECNAV issuance in slightly more than one page with little amplification other than to emphasize "system safety engineering particularly in the acquisition phase of new weapon systems, to eliminate hazards and reduce retrofit safety actions subsequent to fleet introduction." The office (OP-45) which originated that memorandum is the occupational safety and health focal point within CNO and has no system safety responsibilities.

It should be noted that this example of system safety policy being obscured in offices that have only personnel safety responsibilities could

be a reflection of what has gone on at OSD in recent years. If so, it illustrates the importance of OSD's safety image on safety policy in the departments.

One more example of the Navy's apparent assessment of system safety in the management context is the curriculum of the NAVAIR Executive Management course. This program is used to introduce NAVAIR supervisors or prospective supervisors to the scope of NAVAIR activity. System safety is not covered unless questions are presented to speakers describing such topics as reliability and maintainability, which do have scheduled periods.

Does the Navy recognize these problems? The answer is a qualified yes. To illustrate, consider the working-level NAVAIR system safety coordination meeting held in January 1982 [10]. Numerous problems were recognized and solutions suggested, but progress has been difficult to see. Another meeting was held in December 1982 at which industry was asked to critique NAVAIR's system safety programs. It began with a strong endorsement of system safety from the Commander of NAVAIR. Participants were enthusiastic, and NAVAIR should be commended for inviting the criticism that, indeed, was forthcoming. The chief result of that meeting was that the senior-level safety people at NAVAIR, NSC, and OP-09F actively began talking about ways to strengthen system safety.

Within the past year, a system safety function was established at the Naval Air Test Center (NATC), Patuxent River, Maryland. An overall Director of Safety was appointed reporting to the NATC Commander. It appears that the action was precipitated by a series of flight-test center accidents which received critical review from NAVAIR headquarters rather than from any particular recognition of a generic system safety problem in the Navy.

Other attempts by the Navy to correct its system safety management problems include NSC's efforts to get design safety and system safety management guidelines published and AIR-516C's initiative in getting personnel assigned from Naval Air Engineering Center (NAEC) and contracting for outside assistance. A specific effort is underway to have system safety personnel assigned at the NARFs. An F-18 System Safety Management Plan was developed and released 7 September 1982. Finally, the Navy was the only department to present system safety objectives for 1983 at the Spring MBO meeting.

#### SUMMARY

The main problem with the Navy's management of system safety is that existing directives are not being aggressively implemented. The working-level people obviously are trying, but the necessary resources, leadership, and power base both within and above NAVAIR are missing. The organizational uncertainties within NAVAIR, especially the ambiguous role of AIR-516C, also probably limit the effectiveness of their system safety programs. Other than the NSC, there is no system safety spokesman in the Navy above the working levels in NAVAIR. The NSC's role in system safety has not been recognized sufficiently in terms of need and scope.

## 5. U.S. AIR FORCE

### POLICIES AND MANAGEMENT SUPPORT

Of the three Departments, the Air Force has played the predominant role in developing and implementing system safety. It began by introducing formalized system safety engineering specifications into ballistic missile systems in the early 1960s, then applied them to aircraft and other systems later on when the Army and Navy came aboard and MIL-STD-882A was first issued in 1969. Air Force support of system safety in weapon system development since then and their activities, such as underwriting relevant programs at the University of Southern California, have been largely responsible for establishing system safety as a discipline.

The top Air Force safety directive is Air Force Regulation (AFR) 127-2, "USAF Mishap Prevention Program," 4 May 1979. It is roughly equivalent to the Army's AR 385-10 and the Navy's OPNAVINST 3750.6N. It is somewhat engineering-oriented in its emphasis on the importance of acquisition phase efforts; however, it clearly stresses life-cycle system safety group activities, the importance of "lessons learned" from the field, and the need for competent staffing throughout the program. It references and otherwise leads into AFR 800-16, which is the key Air Force system safety requirement.

"USAF System Safety Programs," AFR 800-16, 6 June 1979, is in the acquisition series of regulations. Thus, it is considered to be the implementing directive for DoDI 5000.36. The Air Force Inspection and Safety Center (AFISC) at Norton Air Force Base is the office of primary responsibility for the regulation.

AFR 800-16 states the objective of the Air Force system safety program as follows:

To minimize loss of personnel and material resources through mishaps and to preserve the combat capability of the Air Force by ensuring system safety is applied throughout a system life cycle.

This conservation of resources for mission accomplishment approach is consistent with Air Force pronouncements on safety since the early 1950s [11]. System safety is recognized as a way of achieving a safety objective that includes, but goes well beyond, personnel safety.

AFR 800-16 requires all major commands (MAJCOMs) "to establish and conduct or support an effective USAF System Safety Program." This obviously involves the Air Force Systems Command (AFSC) and the Air Force Logistics Command (AFLC). The using commands (Tactical Air Command (TAC), Strategic Air Command (SAC), Military Airlift Command (MAC), etc.) also have specific obligations stated in AFR 800-16, including ensuring attention to safety in Statements of Operational Need (SONs); assessment of safety risks at program initiation; formulation and review of acquisition, operations, and test planning documentation; participation in System Safety Groups; review of Engineering Change Proposals (ECPs); ensuring that "lessons learned" are documented and forwarded; and ensuring that system operational concepts address safety factors. In short, the Air Force makes it clear that an effective system safety program requires participation from every command along the life cycle.

The only shortcoming in AFR 800-16 is its failure to adequately address the Government-furnished equipment (GFE) problem. System safety is to be considered for facilities and even off-the-shelf procurement items in addition to weapon systems. However, materiel procured by the Air Force and mandated into aircraft (i.e., GFE), for example, is not covered in terms of requiring

that someone (contractor or Air Force) be responsible for total system safety integration. This could conceivably be interpreted as an Air Force responsibility, but the regulation is silent on this point.

The AFSC Supplement to AFR 800-16, 20 October 1981, includes explicit direction to program managers regarding their relation to contractors:

Program or project managers will . . . make sure appropriate safety requirements are included in contracts and, during program management reviews, will emphasize safe design with senior contractor management. If program directors convince contractors that safety is part of the program objective rather than just "boilerplate," then contractors will make safe design part of their corporate goals.

The supplement also requires a "network of primary or additional duty system safety engineers . . . [and] at least one Government system safety individual [be] assigned to provide system safety support to each major system safety acquisition." Furthermore, assistance from system safety trained personnel is required from the Air Force Plant Representative Offices (AFPROs).

The AFLC Supplement to AFR 800-16, 13 August 1980, clearly indicates AFLC's awareness of its role in system safety. It begins by pointing out "The major impact of the system safety program within AFLC is on modifying operational systems," but it does not stop there. The Air Logistics Center's System Safety Managers (SSMs) must perform numerous specific tasks not necessarily associated with modifications, including participation in system safety group meetings and review of the transfer of system safety engineering data at Program Management Responsibility Transfer (PMRT).

Strong emphasis on the "lessons learned" is called for as administered through the Air Force Acquisition Logistics Division [12,13]. Very detailed experience and education requirements are cited for system safety personnel. Training in system safety is shown to be important, not only for system safety assignees but also for project management personnel.

The Aeronautical Systems Division supplement to AFR 800-16 further emphasizes its parent ASFC's interpretation, particularly in leaving no doubt as to the role of the SSM at the program/project level. For example, "The System Safety Manager (SSM) position incorporates engineering and management tasks into one function...The Program/Project Manager, along with the SSM, will tailor SSP requirements to fit each acquisition milestone." This supplement also calls for delivery to AFLC of all safety data for each specific contract at PMRT, thus ensuring the transfer of safety knowledge downstream after acquisition.

Over the years, the Air Force has periodically reinforced its commitment to system safety by command directives, in-house safety conferences, briefings to industry, and the like. Typical in this regard was a Headquarters, AFSC dispatch in January 1982 to various acquisition divisions, and specifically to all program managers. Key excerpts included:

We wish to stress the program manager's responsibility to keep system safety engineering a viable, working part of the system engineering process. . . . System safety must be built in, not added on. . . . Place emphasis on safety of flight not only during full scale development but also through production and deployment. . . . The program manager's direct involvement on a day-to-day basis with system engineering tasks related to system safety will continue to be an item of command interest.

This sort of language leaves no doubt as to AFSC's support of system safety.

Examples of in-house conferences in which system safety issues were brought before the right people are the 1983 Worldwide Safety Conference [14] in which MAJCOMs role in the "lessons learned" program and various provisions of AFR 800-16 were discussed; the meeting of the "AFSC Commander's System Safety Policy Group" [15] where prioritized improvements regarding system safety were developed for the AFSC Commander's approval; and a recent "Software System Safety Working Group" meeting conceived by AFSC's System

Safety office. This session was the first of its kind and was very much needed. External presentations regarding Air Force system safety have been made at international symposia such as those of the System Safety Society and at professional committee meetings such as those of the Electronics Industries Association's System Safety Committee (G-48).

Other miscellaneous documents indicate the depth of Air Force system safety efforts. Air Force Flight Test Center (AFFTC) Regulation 127-3, "Safety Planning for AFFTC Test," applies system safety to test programs, where a person from the System Safety Division chairs the Safety Review Board formed to review each test project. An appendix, "Guide for Hazard Identification," includes risk assessment considerations for flight test operations.

The Air Force rightfully gives heavy emphasis to System Safety Group (SSG) activities. A guide to SSG functioning is available, "System Safety Groups," AFSC Pamphlet 800-44, which includes a provision for life cycle representation by all affected commands including AFLC and user commands during the acquisition phases. Typical implementation of the SSG requirement is seen in the "B-1B System Safety Group Charter." Among other things, it indicates the Program Manager or the Deputy will chair the meetings. Such activity was observed during this study and deemed to be highly effective. Safety decisions were made then and there. An unmistakable image of the importance of system safety in the program was conveyed to the contractors.

A unique accident/incident reporting procedure developed for the F-16 was "Message Reporting of F-16 Flight Mishaps," AFR 127-18. It was triggered by a desire of the AFISC system safety office to keep on top of the program. It illustrates the need to tailor each new program's system safety effort to include the operational world's participation.

A relatively unheralded regulation, but a significant one for system safety is "USAF Feedback Policy," AFR 800-13. It calls for a coordinated effort in processing all forms of unwanted occurrences (from simple malfunctions through actual mishaps) to help apply engineering and management experience and avoid repeating past mistakes. It applies to industry as well as Government sources and lays the groundwork for the extensive "lessons learned" program mentioned earlier. The lessons have pertained to management as well as to hardware or engineering, which makes this feedback system unique.

One Air Force process that has raised questions of coordination with system safety is the "Scheduled Maintenance Program" per AFLC/AFSC Regulation 66-35. This regulation sets policy and procedures for a "Reliability Centered Maintenance" (RCM) program -- a life cycle approach to preventive maintenance. It identifies items as "functionally," "structurally," or "maintenance" significant through failure modes and effects analysis (FMEA) and a defined logic process. It is also concerned with procedures as well as hardware.

The regulation mentions the impact the RCM program has on safety; however, there does not seem to be a discrete tie-in to system safety. One example encountered, and quite possibly within the regulation, was that the RCM analysis could start from scratch, so to speak, without benefiting from the various hazard analyses performed earlier under MIL-STD-882A or MIL-STD-785. The regulation does not take into account the difference between FMEAs and system safety hazard analyses. In fact, both approaches are important to the regulation's maintenance safety

objective.<sup>1</sup> Coordination of all these approaches is necessary to achieve safety, reliability, and maintainability objectives.

Finally, mention should be made of two outstanding education/training documents prepared by the System Safety office at AFISC: "A Risk Management Guide for Air Force Operations," issued to encourage more commanders to think in terms of hazard analysis, and "Introduction to System Safety for Program Managers," limited somewhat to system safety engineering but nevertheless a valuable treatise.

#### ORGANIZATION AND STAFFING

The chain of authority for system safety within the Air Force development and logistics commands is readily tracked by the directives cited above: Headquarters to AFSC/AFLC/MAJCOMs to Aeronautical System Division/Air Logistics Division (ASD/AFALD) to individual programs. The Air Force differs from the Army and the Navy in that system safety programs are in place and working at all levels and for the most part, in all phases of the life cycle of major aircraft systems (F-15, F-16, and B-1B).

The Air Force also pays more attention to the functional nature of system safety. The safety organization at ASD is an example. The Chief of Safety (O-6 level, Colonel) reports to the ASD Commander. The office includes several types of safety personnel. Assignments to programs are made from this office, and the Chief can and does serve as a check and balance on the system manager's safety decisions.

---

<sup>1</sup>Hazard analyses are usually characterized by "top-down" approaches, starting with the undesirable event (e.g., a particular kind of accident) and examining what, singularly or in combination, could cause it. Ideally, these analyses include human-error considerations. (See Chapter 7.) FMEAs, on the other hand, are usually single-component-oriented, concerned more with the failure characteristics of one specific part and follow a "bottom-top" approach in assessment of consequences of that particular failure. Human error (or failure) is not implicit in FMEAs.

The AFISC plays a somewhat different role from that of the safety centers in the other Departments. In matters of aviation system safety, of course, the Directorate of Aerospace Safety (DAS) and thereunder the System Safety and Engineering Division (SES) are the main components. Safety in general has been under the Office of the Air Force IG for 30 years, beginning with aviation, expanding to missile programs, and eventually covering all forms of safety. Because of its power base under the IG, AFISC is the maker of safety policy within the Air Force. In aviation system safety, that function trickles down to DAS and SES.

AFISC/DAS/SES gets involved in system safety well beyond policy issues. Some ways have been mentioned already: the "how-to-do system safety" documents and their educational efforts through University of Southern California. Other educational efforts have been significant, not the least of which was the Aerospace Safety and Safety Journal magazines which have highlighted system safety articles for years. Information of the "lessons learned" type has been made available to contractors and development commands early in the acquisition stage for many programs. DAS/SES personnel are regular participants on SSGs. SES has a unique function of monitoring new technology and instituting related safety actions (lasers, hydraulic fluid flammability, software system hazards, etc.). The IG has even been known to intervene personally on matters of a system safety nature, for example, the flight data recorder issue (discussed in Chapter 7).

Staffing remains somewhat of a problem. There are about 96 full-time-equivalent system safety personnel throughout the Air Force, working with all forms of weapon systems. AFSC headquarters has 4 system safety professional positions, ASD has 24, and AFISC/SES has 18 (5 on specific weapon system programs and 13 in related technology areas). Of these personnel, some are

top-notch "old heads," but there is a substantial gap between them and the inexperienced assignees. This results in inability to assure qualified personnel for anything other than the major programs.

The Air Force, like the other Departments, faces a major problem with position description and grade structure for system safety personnel, which will be discussed in the next chapter. The system safety specialist does not have a home within the civil service job description hierarchy. The job classification people (and many managers) do not appreciate that a system safety program can readily use personnel without engineering degrees, especially those with solid operational safety or maintenance experience, and that system safety management is far different from personnel safety management. GS-12 seems to be the highest grade a civilian can reach as a system safety specialist (on a given program or even monitoring several programs) without supervising a number of people. This leads to instability of civilian personnel assigned to a program. There is a related problem on the military side because career benefits from safety assignments are questionable.

#### PRACTICES

If one were to choose the characteristic most important to the Air Force system safety effort, it would be longstanding management support from the highest levels down to and including program/project management. In acquisition management, what stands out is their emphasis on safety tasks identified in the work breakdown structure of a given program. Without this, system safety management by either the contractor or the government is not as effective as it could or should be.

The Air Force, like the other Departments, has fiscal constraints which sometimes place safety improvements in jeopardy. For example, at this writing, the B-1B program does not include a crash-survivable flight data recorder

(FDR). It was in the predecessor B-1A but was not included in the B-1B baseline in the interest of cost savings. For reasons that are explained more in Chapter 7, this management decision is open to serious question.

A few other Air Force problems were noted. These include the somewhat loose life cycle coordination of system safety engineering, logistics, and operational activities. For example, not all operational commands have issued supplements to AFR 800-16.

Neither AFSC nor AFLC has an effective system for reasonably identifying and tracking safety modification costs. AFSC Form 318 and comparable AFLC forms do not identify safety change total costs. Even with the unwarranted assumption that the "safety" changes were classified uniformly, one must back-track through each ECP and Class IV-A modification file to gain meaningful data. The problem goes back to the configuration control military standard, which will be discussed in the next chapter.

Finally, one still occasionally hears of system safety only in design safety terms [16] -- not often, perhaps, but enough to know that the total scope of system safety is not yet perfectly understood.

#### SUMMARY

Despite the above shortcomings, the Air Force system safety program continues to be a model worth examining by the other Departments and, indeed, by other aviation or non-aviation activities interested in accident prevention.

The Air Force has seemed willing to commit resources, including training and assignment of "blue suit" personnel to system safety. This commitment demonstrates to their contractors that safety is important to the Air Force. It also fosters a command emphasis on safety as an integral part of improved mission effectiveness.

Air Force top management support of system safety has not gone unnoticed by contractors. They now seem more than willing to include system safety tasks, not as "window dressing" but as a meaningful activity.

## 6. JOINT SERVICES ACTIVITIES

### THE RELATIONSHIP BETWEEN JSSC AND SOHP

The annual JSSC sponsored by the safety centers coordinates safety activities. It was described recently as "an unchartered, informal conference of professionals [17]," providing an exchange of ideas in a forum where attendees are highly motivated towards accident prevention. Active for over two decades, the JSSC began in the aviation/aerospace field and expanded as the roles of the centers expanded. Members of the OSD SOHP have attended regularly, and representatives of other Government safety agencies and industry representatives are invited to attend.

The safety center commanders meet as a separate group as well as attend the plenary sessions. Several panels constitute the working groups, one of which is the System Safety Panel (JSSC/SSP) which meets three or four times a year. Major JSSC efforts over the years include standardization of accident definitions and accounting practices, development of a common medical officer's report data coding form, and development of policy on the privilege status of mishap reports.

Typical recent JSSC/SSP projects have been revisions to MIL-STD-882A, development of a laser safety standard, assistance to SOHP in developing DoDI 5000.36, coordination with the Army on its development of an indoctrination film aimed at project managers, and liaison with the Electronic Industries Association's System Safety Committee. The MIL-STD-882A revisions are of particular significance since all the Departments' system safety programs are related to that standard. Other changes are underway, such as transition to a task format compatible with more detailed work breakdown

requirements, introduction of human error assumptions into hazard analyses, coordination of data item descriptions, and others.

JSSC and SOHP have developed an excellent working relationship. Representatives from SOHP can and do influence tasks undertaken by JSSC. Conversely, SOHP is the one office at OSD to which JSSC safety matters can be funneled directly.

The JSSC/SSP has been particularly helpful to SOHP as a communications link. They have been most willing to solicit views from the SOHP Director in the past and have offered to examine questions posed by him. Certainly the panel was extremely valuable during this study.

Mention of this relationship between SOHP and JSSC serves as a means of introducing several similarities and differences among the Departments relative to system safety which were not necessarily apparent from the preceding chapters. Observations at JSSC meetings and conversations with attendees confirmed or actually focused attention on common issues which might otherwise have been passed over as peculiar to a given Department.

#### SOME SIMILARITIES IN THE DEPARTMENTS' APPROACHES TO SYSTEM SAFETY

One can find both positive and negative similarities in the Departments' approaches to system safety. On the positive side, the safety policies of the Army, Navy, and Air Force all identify the purpose of safety efforts as not only to protect personnel from accidental injury or death but also to protect other DoD resources as well. This may sound like a truism to people familiar with military safety activities, but to others the application of "safety" to inanimate objects is novel. The Departments have rightfully and plainly indicated that they are in the safety business to conserve all parts of the "system." This is a necessary foundation for system safety.

Second, all the Departments recognize the necessity for command/management attention to safety. They also agree that safety specialization belongs in their organizations in the role of assistance to command/management. This, too, is essential, because without a recognized organizational role, no system safety technology could reasonably be applied.

Third, all Departments have endorsed system safety policy as typified by DoDI 5000.36. Their regulations say it. There is activity, although to varying levels, among all three. Thus, there is no argument that system safety is in the military environment to stay.

Fourth, the military aviation accident rate has generally improved over time. At first, the improvement was rapid, as the importance of specialized attention to operational safety was recognized. In recent years, the rate of improvement has slowed as further gains in operational safety became hard to find and aircraft and overall system complexity have increased. The challenge for system safety in aircraft programs is to continue improving accident rates through emphasis on safety during the acquisition phase.

On the negative side of the similarities among the Departments, no clear policy seems to relate system safety to the other safeties. Organizationally, this is confusing and misleading. If system safety is not identified in the proper context with other safeties, numerous related problems develop, not the least of which involves staffing.

Similarly, no evidence has been seen that any of the Departments has evaluated and determined what the balance is or should be in resource expenditures for all of aviation safety (including its system safety component) as compared to other safety activities. Without analysis of some baseline data, resource expenditures may be based more on emotion and politics than on national defense and the public interest.

Although this study has not included any detailed review of that question, the cost of aviation accidents is significantly higher than all other DoD accident/occupational illness costs combined. The proper allocation of resources is unknown, but what is missing is an assessment of DoD's investment in accident prevention, at least in terms of staff assigned to and/or working in various safety activities. This is needed in far more detail than was shown in the recent MBO reviews. OSD and Service management needs more of this investment side of the accident prevention equation to place system safety (aviation or otherwise) and other safeties in proper perspective.

A common problem, at least until very recently, has been a general lack of understanding of the life cycle connotations of system safety or the erroneous identification of system safety only with "engineering." For example, there was no contractor safety support for "mature" systems (e.g., C-5 and A-7) even though they entered different use environments. Coordination of system safety efforts considering engineering, test, logistics, and operational activities has been limited within all three Departments. Feedback loops (from the field to acquisition and vice versa) are in their embryonic stage.

Coordination between traditional flight (operational) safety activities and system safety engineering activities also needs improvement. For example, accident/incident investigations are seldom conducted using system safety information such as hazard analyses. Accident/ incident investigations and hazard analyses are identical in principle except that one is done after-the-fact and the other is done before-the-fact. Obviously, the two activities should be coordinated. Furthermore, investigations should examine breakdowns in the system safety program whether caused by engineering or management. Today, no guidance or practice is in place anywhere to use accident/incident

investigation results to evaluate the adequacy of system safety programs or to identify where they broke down and how they might be improved.

Revisions to MIL-STD-882A are underway to place system safety requirements in more of a task format. Indeed, in some contracts, the work breakdown structure has been tailored to detail system safety tasks sufficiently to allow their tracking as part of the safety management process. This is an all-Department problem, however, because of the limitations of the current "Work Breakdown Structure for Defense Materiel Items," MIL-STD-881A. This standard is "a product-oriented family tree composed of hardware, services and data which results from project engineering efforts during development and production which completely defines the program." System safety is presumably a "service," and systems engineering integrates safety, reliability, maintainability, etc. at "Level 3" according to MIL-STD-881A. The difficulty is that system safety is "lumped-in" with other functions where funding could be diverted. There is a need to either modify MIL-STD-881A to identify system safety separately or ensure that tailoring of the work breakdown structure is routinely accomplished with respect to system safety tasks.

A comparable problem exists regarding provisions of another DoD standard, "Configuration Control, Engineering Changes, Deviations and Waivers," MIL-STD-480. Under this standard, proposed modifications are supposed to be coded "safety" if the change "is required to eliminate a hazardous condition." The difficulties are that the definition of "hazardous condition" is broad and, more importantly, no guidance is available as to who finally determines the classification. The standard implies that a "safety" classification is a design deficiency which, under most contracts, means that the contractor must absorb costs. In any event, no consistency in classifying safety changes was found at the development commands. As a result, there is no effective data

base for the number and kinds of safety changes being made. This fact, coupled with forms that do not necessarily tabulate all cost factors in one place, ensures that the value of the existing information on modifications is minimal.

Still another problem involves GFE. Comments heard at the Navy system safety meeting last December and conversations with Army contractor personnel indicate that this problem is DoD-wide. No clear policy appears anywhere to assure total system integration of hazard analyses for contractor and GFE. Attempts might be made in MIL-STD-882A to convey the need for such integration, but the scope of the standard cannot really define the Governments' obligations. The issue becomes one of program management policy and direction.

Finally, no evidence has been seen that safety is a consideration in Service System Acquisition Review Councils (SARCs) let alone DSARCs. This is not surprising considering the mild requirement in DoDI 5000.2 that the Integrated Program Summary will address safety only "as required." The pre-DSARC briefings now being arranged by SOHP is a step towards changing this situation.

#### SOME DIFFERENCES IN THE DEPARTMENTS' APPROACHES TO SYSTEM SAFETY

Certain differences obviously exist in the Departments' approaches to system safety and a discussion of some which may not have been apparent earlier may identify areas for possible corrective action. This is not to imply that what works for one Department would necessarily work for another. There are always some advantages and some disadvantages, and tradeoffs are usually required.

#### Placement And Role Of Safety Activities

In the Air Force, a system safety officer is assigned, for example, from the staff safety office in the Aeronautical Systems Division of AFSC to a

program office, where he reports directly to the program manager (System Program Office (SPO) Director). In the Army, the usual situation is for the System Safety Office (a staff function) in AVRADCOM to provide technical support to the program office via an individual within the program office who is designated collateral responsibility for safety. The Navy operates similar to the Army in that a safety office in NAVAIR (Air 516C) provides technical support to the "principal for safety," designated by the program manager. Thus, the major difference observed is that the Air Force assigns the system safety specialist directly to the program manager, whereas the Army and Navy do not. This difference suggests that in the Air Force the system safety specialist is more likely to be directly involved in the decisionmaking process than he is in the Army or Navy.

It is also interesting to note in passing the organizational positions of the respective safety centers. In the Army, the safety center reports to the Director of Army Safety, a staff function under the DCSPER. The Commander of the NSC reports to the CNO through the VCNO. In the Air Force, the safety center is part of the AFISC, under the IG. Each of these organizational arrangements has its good features and logical appeal: (1) personnel safety is the overriding concern in the Army, (2) the NSC reports at the highest possible level, and (3) the Air Force safety center enjoys the independence and influence traditionally associated with inspection functions.

#### ALLOCATION OF PERSONNEL, CLASSIFICATION, AND TRAINING

Again, a spectrum of approaches exists among the Services, this time involving the mix of civilian and military officers in influential system safety positions. The Air Force tends to have a preponderance of military officers directing their system safety efforts. The Navy tends to have more civilians. The Army is somewhere in between.

The numbers of aviation system safety personnel within the Departments can vary depending on the definitions one chooses. A narrow definition would be simply persons with "system safety," or something equivalent, in their title. The broadest definition would be all persons with aviation safety titles, including aviation/flying safety officers or the equivalent. Does aviation system safety properly include all personnel who apply specialized accident prevention knowledge over the life cycle of the systems? The answer rests upon whether one wants input from all aviation safety personnel or only from persons assigned to system safety as defined by current regulations or referred to in work resulting from MIL-STD-882A's application to aircraft.

Using the latter definition, the Army has about 18-20 aviation system safety personnel, mostly in AVRADCOM. The Navy has about the same number, mostly in NAVAIR. The Air Force has probably about 45-50 in aviation, 24 of whom are in the Aeronautical Systems Division of AFSC. This places the total number of aviation system safety personnel within DoD at something under 100 persons, counting both military and civilians.<sup>1</sup>

These data are only approximations of actual plus full-time-equivalent personnel since there is no uniform way of counting these people. When it was attempted in one Department, the assessment seemed to have been "done with mirrors," according to a senior civilian system safety official. The criteria for what constitutes system safety efforts have simply not been sufficiently defined or understood.

---

<sup>1</sup>An approximation of the total number of system safety personnel assigned to all kinds of weapon systems would be 50 in the Army, 35 in the Navy, and 120 in the Air Force. The 1976 DoD safety management study showed total "military aviation safety personnel" to be 350 in the Army, 400 in the Navy, and 1,100 in the Air Force. No identification was made of system safety personnel contained within those numbers, if any.

Using these data as outside limits of Government aviation system safety personnel costs, it can be shown that probably less than \$10 million annually is spent for this purpose. It also represents roughly 5-10 percent of the total budget for all DoD aviation safety personnel.

Numbers of personnel are one thing; actual qualifications and experience is something else. With the exception of one unpublished study by the Air Force, this subject has not been addressed; hence, little can be said here. What has been apparent, however, is the uselessness of civil-service position descriptions and job standards for determining what is going on in system safety or, for that matter, establishing a reasonable grade structure.

GS-803 is a "Safety Engineer" classification, but it does not allow for qualification of those who are needed at various phases of the life cycle who may not have an engineering degree. GS-018 is a "Safety Manager" whose qualification requirements are entirely oriented towards occupational safety and health. Neither classification permits someone with system safety training and broad experience to be hired at a reasonable grade or progress in grade sufficiently to remain in the field.

Several stories were recounted to the study team about personnel being forced to leave system safety positions because of these problems. Industry faced up to this problem years ago. They established a variety of system safety position descriptions, allowing for engineering, test, operational experience, etc. They also adopted a non-supervisory "member of the technical staff" classification to retain people who were not supervisors but had essential experience.

The problem of position classification was taken to the Office of Personnel Management (OPM) without success by a committee of the System Safety Society in 1980. It was also reviewed by JSSC/SSP early this year. Inquiries

made during this study suggested that OPM could not be bothered with the matter since there are "obviously not enough system safety positions to warrant an occupational study." Absence of effective civil service position descriptions and grade structure is critical to the improvement of system safety efforts in DoD -- aviation or otherwise.

There is a similar problem in staffing of system safety positions with military personnel. Safety assignments in the military have generally not been considered as career enhancing. Safety is a small activity and usually does not allow demonstration of management capabilities in many of its assignments. It is fundamentally a staff rather than a decisionmaking position. If the importance to management of system safety becomes better recognized, and if safety supervision is broadened to cover all safeties (as the trend seems to be), the military safety career will become more attractive.

Education and training of system safety personnel within the Departments vary widely. The Army has had a short, basic system safety course for 13 years at the DARCOM Field Activity, Charlestown, Indiana, and it is apparently very successful. Until a few years ago, DARCOM had a master's program (at the Red River Army Depot, Texarkana, Texas) with a safety emphasis which provided excellent training for those entering or advancing within the safety field. It apparently was the victim of budget cutbacks, and some efforts are underway to get it reinstated.

The Navy has had a system safety course at the Navy Postgraduate School for about five years. It is a required part of the Aeronautical Engineering master's program. About 50-60 students take the course each year, about one-third of whom come from outside the program. Faculty at the school have also provided a 16-hour system safety indoctrination course at a few bases in recent years. Navy headquarters contracted for one- to two-week session of

system safety lectures at numerous bases for several years, patterned after the short course offered by George Washington University, but that program no longer exists.

The Air Force has provided system safety courses at University of Southern California since the mid-1960s, currently attended by about 70-80 persons per year. This program has contributed a great deal to the development of Air Force system safety personnel, but it has recently been criticized for being too analytical and operations-research-oriented. As a result, more emphasis is being given to acquisition management and presumably the full life-cycle scope of system safety. The Air Force Institute of Technology also provides system safety indoctrination by distributing relevant material in some of its programs.

Some 200-300 military and DoD civilian personnel have taken a master's program in safety from University of Southern California through courses given on campus, at military sites, and in Washington, D.C. System safety is a major part of that curriculum. Unfortunately, few of the graduates are in Government safety positions. Also, many students have been sent regularly to a fault tree hazard analysis course originally developed at the University of Washington.

The Defense Systems Management College introduces system safety in their program management course for prospective weapon system managers. Due to time constraints, however, this effort which is only about a year old, entails only a single 30-60-minute lecture.

#### SUMMARY

Through the medium of JSSC, the Army, Navy, and Air Force have been coordinating well in advancing safety overall and system safety in particular. The common problems described in this chapter would seem

to be readily amenable to resolution with JSSC's help. These include the need to:

- Place system safety in better perspective to the other safeties.
- Understand and perhaps affect a better balance of effort between aviation system safety and other areas.
- Understand and promote the life cycle meaning of system safety better.
- Develop an improved safety management data base regarding aircraft safety modifications.
- Ensure sufficient identification of system safety tasks in program work breakdown structures to serve program implementation and monitoring needs.
- Integrate GFE into the hazard analysis process more effectively.
- Improve the consideration of system safety in the SARC processes.

An additional and particularly critical problem facing all the Departments is the attainment, development, and retention of effective system safety personnel. It can be remedied by a better understanding of system safety, by organizational alignments that effectively group all the safeties together, and by recognition from personnel specialists of system safety as a distinct career field.

## 7. SPECIAL ISSUES

During this study many discussions took place with individuals representing a broad cross section of the military aviation community. Certain issues arose consistently which were not necessarily within the initial bounds of the study. They have been mentioned occasionally in previous chapters; however, they merit separate discussion here because of their actual or probable impact on system safety efforts. All are of significance to DoD management.

These special issues are:

- Contract Incentives. How can manufacturers be motivated through the contracting process to give adequate emphasis to system safety?
- Life Cycle Safety Benefits From New Technology. How can newly available technology improve safety when the benefits are measured in life cycle terms?
- Human Factors and Safety. How can more progress be made in avoiding "human error" accidents?
- Software System Safety. How can this relatively new problem be controlled before it gets further out of hand?
- Safety Information Exchange in a Litigious Society. How can the communication of safety information be maintained let alone improved, in the presence of increasing aviation accident litigation?

### CONTRACT INCENTIVES

The principles underlying contract incentives are hardly new. The objective is to motivate contractors to apply their best efforts to achieve certain desired goals (e.g., relative to performance, cost, and schedule). The Government gains, and the contractor is rewarded monetarily in the characteristic manner of the free enterprise system.

DoD has had experience with this approach in many areas, including reliability and maintainability (R&M). Improvements in R&M have resulted as the requirements became more definitive and incentives were provided in the

contracts. Usually, "more definitive" meant "quantitative," and that is where the question arises as to how to obtain similar results in safety.

Safety is not as amenable to quantitative treatment as is R&M. Accidents are almost without exception caused by multiple factors and the relative contribution of each is usually not clear. Moreover, the frequency of accidents, for any particular model of aircraft and cause or group of causes (such as those which might be attributable to design or production deficiencies), is probably not great enough to provide statistically precise assessments of whether or not the aircraft has met a specified accident rate. Therefore, any attempt to incentivize contractors via provisions based on a specified accident rate would be complicated and impractical, and would likely result in difficult contract negotiations, protests, and litigation. A better approach would be to use award fees for the performance of system safety tasks. Under an award fee type contract, the contractor has the potential for earning an additional profit (above and beyond the fee negotiated on the basic contract, for instance cost-plus-fixed-fee), depending upon the extent to which he excels in the performance of specified tasks. The award fee, thus, is an added bonus of which the contractor may be awarded all, some, or none.

The fee itself is usually part of an overall package of possible awards which may not really be large in terms of the entire contract (low hundreds of thousands of dollars for awards on a major project), but is pure profit for the contractor. Government personnel, usually a small panel advising a "fee determining official," will evaluate how well the contractor performs the designated tasks and an appropriate fee is awarded.

The concept is being used successfully by the USAF/AFSC Space Division for system safety contractors. These contracts are complete with award fee criteria in terms of award fee percentages allocated for differing levels of

performance, definitions of differing levels of performance, time periods for evaluation and award fee spread throughout the life cycle, and criteria for assessing each period.

It goes without saying that the successful use of award fees for the performance of system safety tasks depends heavily upon the ability to specify the detailed tasks against which performance is to be judged. It appears that revisions to MIL-STD-882A now underway will result in a task-type format (patterned after that which is used in reliability standards) which will lend itself to better definition and specificity of system safety tasks [18].

The award fee concept has life-cycle safety cost implications: that is, spend now, save later. Of concern, however, is that no evidence was encountered during this study to suggest that life cycle costing in the acquisition process recognizes the benefits of accident prevention through the system safety process. A similar finding was made by the 1976 DoD safety study group.

Attrition is factored into the planned production quantity to compensate for losses at any given time in the life of the aircraft based upon past performance of similar weapon systems. No savings analysis is used, however, most likely because no safety effectiveness criteria have yet been incorporated into the life cycle costing process.<sup>1</sup>

Clearly, a policy change indicating the need for safety input to life cycle costing appears warranted. Common sense and any test of reasonableness show the cost of a system safety program (Government and contractor combined) would be but a fraction of the cost of a single modern high-performance aircraft. (Award fees would add little to that.)

---

<sup>1</sup>The Electronics Industries Association's System Safety Committee (G-48), has developed a bulletin, "Impact of System Safety on Aircraft Life Cycle Costs," which is available to "assist procurement agencies concerned with establishing requirements for Life Cycle Cost."

#### LIFE CYCLE BENEFITS FROM NEW TECHNOLOGY

It has long been realized that the technology which has improved aircraft design has produced advances in aviation safety. It has also produced new hazards. The operation of some systems is so complex that it often defies the understanding of all but a few experts.

Safety technology, like other technologies, has advanced. Methodologies have been developed (e.g., hazard analyses and accident investigation techniques), and safety systems of at least one variety, escape and survival, have become commonplace (e.g., ejection seats). Safety systems, for purposes of this discussion, are defined as those hardware items whose sole or principal purpose is the prevention of accidents or deaths/injuries related thereto.

Until a recent meeting cosponsored by SOHP and OUSDRE, communication between the system advanced technology community and safety specialists was minimal. Clearly, the safety people must anticipate new or changing hazard areas and prepare for them. Equally clear, the research and development people should be aware of what can be expected to give safety problems in the future and use their knowledge to develop and apply safety systems.

The FDR offers an unfortunate case study of a safety system. Also known variously as a "flight incident recorder," "crash-survivable flight data recording system," and "Accident Information Retrieval System" (AIRS), its purpose is primarily to recover information of benefit to accident investigation. It can also be combined with a Crash Position Locator (CPL) or Crash Position Indicator (CPI) to produce what the Navy once called a Universal Locator Airborne Integrated Data System (ULAIDS). Sometimes, and preferably, an FDR can be combined with other on-board data systems such as a Maintenance Signal Data Recording System (MSRDS) or a Survivable Flight Control Memory Function (found in the F-16). This saves space and weight.

For over a decade there has been an overwhelming desire within the military safety community for a locatable, crash-survivable FDR. Safety experts saw benefits from FDRs during accident investigations conducted by the National Transportation Safety Board (NTSB) and its predecessor, the Civil Aeronautics Board, in civil aviation since the 1960s. A 1973 CNO policy statement resulted in a design specification requirement for FDRs [19]. An Air Force Chief of Staff policy statement in 1973 led to at least three funded feasibility studies for FDRs. AFISC eventually produced a Statement of Operational Need (SON) in 1979.

The Army and Navy produced their own systems (AIRS and ULAIDS) and installed them on a limited number of aircraft. Off-the-shelf civil systems were installed in some military transports despite the fact that NTSB has argued for years that current and forecastable technology would allow installation of much better systems in civil aircraft. A tri-Service recorder specification has been under development for several years. The Navy independently produced their own specification, MIL-STD-2142(AD), 18 June 1982.

What is the status of FDRs today, especially with respect to DoD's most advanced (and expensive) aircraft? Following a decision reached just early this year and after considerable personal pressure from the Air Force IG, a system is going into the F-16. Indeed, the Vice Chief of Staff directed on 15 November 1982 that all aircraft programs will have an FDR unless a waiver is granted by the Chief of Research and Development of the Air Staff. The other Departments and their contractors are going to derive what they can from the F-16 FDR and evaluate it for incorporation in some of the other current high performance aircraft such as the F-18. No plans exist for FDR incorporation in the B-1B as of the time of this study. The tri-service standardization effort is going forward based on what will be done with the F-16/F-18.

Why did an FDR not find its way into current aircraft more expeditiously and more cost efficiently? The answers are not as simple as they might appear even given the fact that the technology for these systems has been available for several years.

Generally speaking, support from the operational community was, at best, less than enthusiastic about equipment that did not allow them to fly higher, faster, farther with more ordnance, etc. Program managers, at least initially, did not recognize the available advances in technology which made weight and cost "penalties" minimal if the systems were designed-in at the beginning of the program, especially in concert with other on-board instrumentation systems.

Decisionmakers failed to recognize the cost avoidance benefits associated with FDRs. The impact of program delays due to unexplained accidents can be avoided. This becomes particularly critical if the accidents occur during test and evaluation or in early operational use. Investigation costs and sometimes needless modification and retrofit costs occur. None of these can be minimized without accurate investigative findings. Loss of foreign military sales (if not the entire program) could occur if early accidents are not explained satisfactorily.

Another major factor in delaying FDR incorporation was cost constraints which put long-term safety benefits in a very low priority compared to steps that could be taken to solve immediate problems.

The optimistic attempts to standardize an FDR system for all Departments also delayed matters. With that effort going on, the perfect excuse was at hand for program managers to defer decisions affecting their airplanes. The problem was that there were genuine differences in operational requirements and aircraft configuration. For example, the Navy needed ejectable,

locator-equipped FDRs because of their sea-based operations. These would not necessarily be required for the Army and the Air Force. The crash hardening for a helicopter system need not be the same as for a fighter.

Most important of all was the absence of any DoD precedent or policy speaking to the need to consider the benefits of safety systems over a program's life cycle. Without this, program managers are going to emphasize those requirements against which their performance will be measured in the existing phase of system development. Few program decisionmakers appreciate the cost and mission readiness improvements that can result from effective, more timely use of accident prevention systems such as the FDR.

The FDR problem is even more critical today. Following discussion of the subject at the OUSDRE-SOHP Safety Technology meeting, Rear Admiral Steele of the NSC, stated that five factors must be addressed (when considering aircraft mishap analysis and the need for FDRs):

- The continuing high percentage of unresolved mishap causal factors (13 percent in a recent year for the Navy).
- Rapidly emerging computerized control and display technology that is not totally amenable to classic mishap investigation techniques.
- A high percentage of mishap causal factors directly related to human factors (and the difficulty in the investigation thereof).
- The rapidly accelerating cost of aircraft.
- An increased use of unique materials, i.e., composites which are not totally amenable to classic material failure analysis techniques [20].

A similar situation exists with the Ground Proximity Warning System (GPWS). Extraordinary reduction in civil air accidents has occurred since introduction of GPWS in the early to mid-1970s, yet the pattern set by the FDR is seemingly being followed by the GPWS.

A CNO message of January 1978 identified a GPWS requirement which was initially applied to the C-9B and H-53. An Air Force SON has been prepared by

TAC and presented to the Air Staff. The Air Force is sponsoring some limited research to identify GPWS benefits more precisely for high performance aircraft. The Navy has been doing some planning for a "Low Altitude Safety Alert System" (LASAS) following a request from CNO in July 1982 to "plan your options [21]." Those few systems incorporated in military aircraft seem to be the results of off-the-shelf buys rather than a structured program objective. There is good reason to believe that a large percentage of accidents in military aircraft, including relatively high performance aircraft, are good candidates for accident avoidance using a GPWS system, yet the subject has not had appreciable inter-Department discussion, and a safety systems implementation policy does not exist.

#### HUMAN FACTORS AND SYSTEM SAFETY

The challenge to reduce human error in aircraft accidents faces everyone in the air safety field today. But what do we mean by human factors in the system safety context? These are the key elements:

- Personnel selection, assignment, and performance;
- Design and test of the aircraft from the view of human engineering; especially cockpit layout, controls and displays, hardware development compatible with human limitations, and allocation of workload;
- System biomedical considerations;
- Procedure development;
- Training;
- Operational personnel situational awareness and motivation;
- Emergency escape, search, and survival.

"Human Factors Engineering", as part of the acquisition process, is usually concerned with all of the elements above. A human factors "task analysis," a task description and analytical process, is the initial and main thrust of most human factors engineering work and is analogous to hazard

analysis in system safety. From the task analysis flow considerations of the number and types of personnel required, their training, the hardware design for effective human interface, procedures, etc. Obviously this process would offer opportunities to identify human error potential.

Were one to examine the total scope of human error hazard analysis, one would see a relationship developing that goes beyond human factors or system safety requirements per se [22]. Human error analysis begins with task analysis, hopefully undertaken concurrently with system design. At virtually the same time, various hazard analyses specified in MIL-STD-882A are begun which, like the task analyses at this point, are predominantly on paper. These analyses include preliminary hazard analysis, system/subsystem hazard analysis, and operating and support hazard analysis. Other opportunities arrive further along the system life cycle. These include full and part task simulation, test and evaluation programs, and operational experience. Ideally, these should all be integrated into a total human error hazard analysis program.

There appears to be little or no integration of safety and human factors analyses during a system's life cycle. Of particular concern is the near total absence of dialogue, or coordination between system safety and human factors personnel in attacking the human error problem. The key military specifications, MIL-STD-882A and MIL-H-46855B (military handbook) [23] contain only the slightest cross-reference to one another. Cross-referencing is similarly absent in most of the implementing regulations. Few personnel interviewed in each field had seen or heard of the other field's basic specification. Human factors personnel rarely participate in SSGs. What coordination does occur (except at the manufacturers) too often occurs well downstream in the acquisition cycle.

Closely allied to the communication problem is the perceived "ivory tower" role of the human factors people, many of whom appear more disposed towards research than problem-solving at the project level. Similarly, some system safety personnel project a "crusader" image that can detract from their effectiveness. Both groups tend to be attached to a single discipline (usually psychology in the human factors engineering case), when proper human factors work, like system safety, requires an interdisciplinary approach.

Another major problem is the difficulty of investigating human factors in accidents [24,25]. Moreover, programs are limited for incident reporting and investigation within DoD; that is, for voluntary reporting of non-damage events involving human error. The Departments have made some efforts in this direction for many years (e.g., the Air Force's Operational Hazard Report system and the Navy's "Anymouse" system) but these programs do not seem to be very active today.

A few years ago, civil aviation began an Aviation Safety Reporting System, administered by the NASA for the Federal Aviation Administration (FAA). It is an anonymous, nonretributive approach to incident reporting. The reports are reviewed by a selected, interdisciplinary team of experts concentrating on human factors problems. It has been quite successful and would seem to be adaptable to military aviation.

The problems described above have been also recognized by others. Dr. Anchar Zeller, a senior research psychologist at the Air Force DAS for many years has written of the need to reduce human error accidents not only through standard human factors engineering but also through integrated management systems [26]. A Defense Audit Service study in 1980 cited similar findings [27] as did a 1981 study by the Government Accounting Office [28]. An Air Force RFP in 1981 to develop a "Human Oriented Mishap Reduction (HOMR)"

system stated bluntly that:

. . . literature and data regarding the human factors aspects of aircraft mishaps is in a state of disarray . . . [and] there is a wide gap between human factors technology and its practical application.

On the positive side, the ASC has done some excellent work in structuring human factors investigations beyond the traditional medical officers' approach [29]. Also, the Army's management concept for major programs includes essentially a contract between their human factors people and the program office to assure timely input [30].

In addition to Project HOMR, the Air Force has noted in its "System Safety Guide for Program Managers" the need to involve human error in hazard analyses. Other Air Force activities include a "systems application panel" within the F-15 System Program Office which gathered together those staff specialists involved in cockpit design, including safety and human factors personnel. AFSC uses a Human Factors Board, similar to the SSG concept, in their Integrated Logistics Support program.

The Navy has informal human factors working groups on some of its major projects. NAVAIR's "Human Factors Engineering, Master Plan, FY83" (for research) realizes that "Potential hazards in the area of human performance and behavior must also be identified and corrected."

Accidents caused by human error are the prime target for preventive action in military aviation today. Some impressive management practices and research are underway or planned; however, with the exception of Project HOMR, they do not seem to be life-cycle-oriented. Furthermore, coordination between system safety and human factors activities leaves much to be desired, especially during acquisition, more precisely, during hazard analyses.

## SOFTWARE SYSTEM SAFETY

This problem can best be described by recounting a few representative mishaps:

- A wing-mounted missile failed to separate from the launcher after ignition because the external stores sequencing program signaled the rack-retaining mechanism to close before the rocket thrust built up sufficiently to clear the missile from the wing. The aircraft went violently out of control.
- In a fly-by-wire flight control system aircraft, a mechanical malfunction set up an acceleration environment for which the flight control computer was not programmed. The aircraft went out of control and crashed.
- A computer-controlled automatic throttle system malfunctioned, forcing the aircraft off the deck of an aircraft carrier.
- A bomb bay door closed unexpectedly hours after anyone was near its controls when power was reapplied to the airplane due to a computer-controlled circuit "glitch."

These events illustrate a problem which has often been referred to incorrectly as the "software safety" or "software hazard" problem. Nothing is dangerous about "software" itself. The burgeoning computer-based systems of which computer software is but one subsystem and their mechanical or human failures are the real problem. More properly, the "computer-based system" or, alternatively, the "software system safety" problem includes aircraft hardware, computer hardware, aircraft software (e.g., handbooks, procedures, etc.), computer software, and the human element.

Hardware failures stem from the aircraft, its subsystems, or support equipment. Human-induced hazards can, in turn, emanate from the aircraft/support system hardware designer; the computer hardware designer; the manufacturer of any of the hardware; the aircraft operations and maintenance procedures writer; the computer systems analyst, programmer, etc.; the aircrew members (who sometimes function in their own right as systems analysts or programmers in a broad sense); and aircraft maintenance personnel.

The fact remains, a relatively new breed of hazards and associated problems has appeared. They appear primarily in flight control systems, armament control systems, navigation systems, and cockpit displays. They add new dimensions to the human error problem.

Some of the hazards are passive until just the right combination of circumstances arrives (the bomb bay door closing). Some result from the crew's multitude of choices in aircraft system management, often during prioritization of tasks. Conversely, computer-based systems are supposed to relieve pilot workload, but perhaps too much so in some instances, with resultant complacency and/or "lack of situational awareness," which is a broader crew performance problem applicable to both the failure and non-failure modes of the equipment (e.g., navigation or flight management system errors).

New dimensions (including cost) of accident investigations have arrived with computer-based systems or, as stated rather pointedly, "Malfunctioning electronics will not be found in the wreckage [31]." The F-14 carrier deck case resulted in millions of investigation dollars being spent.

The state of the art in resolving these problems is disturbing in that aircraft systems are in operational use without appreciable analysis of software system safety having been done during acquisition. The encouraging side is the recognition that a problem exists and people have started to communicate about it. Only within the past two years has this area received published attention outside of, perhaps, the nuclear safety field. Papers on software safety were first presented at the 1981 System Safety Society biannual meeting. Related research began about that time at the University of California at Irvine with support from the Hughes Corporation. Relevant publications by a European committee allied with their nuclear power industry appeared. The G-48 System Safety Committee formed a subcommittee on software safety.

The NAVAIR's "Human Factors Engineering, Master Plan, FY83" (for research) has a line item concerned with computer software error identification and control. Recently, an Air Force "Software System Safety Working Group" was formed under the auspices of the system safety office at AFISC. For probably the first time, computer science and system safety specialists were gathered together in the same room to exchange views. One result was the planned development of software hazard analysis methods to be included within MIL-STD-882A when appropriate. No plans exist yet to link this group to the JSSC/SSP. This or some comparable undertaking would be desirable.

A NASA system safety representative at the working group meeting related some of the critical experiences they had had during space flight activities. Their software system safety problems have been attacked principally by extensive simulation exercises, which may be the only practical way to analyze for such problems in the near future. No one was aware of any published DoD requirements or guidance documentation in this regard.

The significance of the software safety issue to the objectives of this study rests in the realization that software safety typifies the dynamic nature of aviation technology and the need to continuously monitor such developments in terms of system safety. The STARS program illustrates how an interdisciplinary safety problem can be missed when only personnel of one discipline (computer science) get involved.

In conclusion, software system safety is a relatively new and highly critical area of concern. Its full implications are understood by only a small number of people. Generic analytic and management solutions or controls do not exist, although some concerned professionals from both the system safety and computer science fields are beginning to work on them. This subject should be monitored closely by all DoD safety offices and the JSSC/SSP.

### SAFETY INFORMATION EXCHANGE IN A LITIGIOUS SOCIETY

The perceived threat of litigation following aviation accidents inhibits communication of information that might prevent future accidents. The problem is exemplified by a statement in OPNAVINST 3750.6N, "the concept of privilege pervades the Naval Aviation Safety Program." That statement is there because the Navy, like the other Departments, has had to restrict dissemination of accident reports to ensure that it will obtain information that will help prevent accidents, yet not expose witnesses and the Navy's own analytical processes to litigation.

This is not a new problem, just a larger one with more ramifications as system safety efforts grow. Heretofore, the impact of potential litigation was only on mishap investigation information. Now it also concerns hazard analyses, minutes of system safety group meetings, safety action reports, etc.

Access to "lessons learned" at safety centers is being limited and/or delayed due to administrative safeguards deemed necessary to protect the privilege status of mishap reports. This is unfortunate since safety analysts often need to review original reports as well as summary information or statistical data. Contractors have been discouraged from asking for information because of delays in response time.

Installation of computer terminals at contractor or Government facilities that allow access to safety center data have been delayed, not only because of limited funds but also because no acceptable means of protecting privileged information has been found. Contractors are limiting their retention of safety data, malfunction records, etc., for fear of being forced to produce them on discovery during lawsuits.

Contractors may limit their system safety efforts if those efforts increase their liability exposure. Such exposure has already increased under

strict liability codes and court decisions which suggest contractors are liable if they know of a hazard and "fail to warn." Some efforts underway to have contractors "certify" safety levels via specially qualified and designated personnel may further increase their liability under implied warranty principles.

Contractors were placed in a highly vulnerable position by the 1977 U.S. Supreme Court decision in Stencel Aero Engineering Corp. vs. United States [32]. The main issue in that case was Government indemnification of contractors for damages paid to Government employees injured in accidents. The U.S. Supreme Court held that the Federal Tort Claims Act precludes the United States from indemnifying such third parties (the contractors). The net effect was more subtle. Since the Government could not shield its contractors even if it wanted to, liability fell to the contractor even for designs approved by the Government. Stencel strengthened past decisions (notably Boeing Airplane Co. vs. Brown in 1961 [33]) holding, in effect, that manufacturers are still liable in accidents involving unmodified aircraft even though they realized the need for the change, modified the design, and adhered to change incorporation timing directions from the customer, the U.S. Government. The principles of strict liability in tort were held to apply without intervening culpability by the Government; that is, if the hazard existed in the design and remained effectively unchanged until the injury producing event, the manufacturer was held liable. Faced with this and other economic or reputation considerations, manufacturers were reluctant to come forward with safety fixes.

Fortunately for manufacturers and probably the Government in the long run, an April 1983 decision by the Ninth Circuit Court of Appeals held a somewhat contrary view to Stencel. In the case of McKay vs. Rockwell [34],

the court took the position that military aircraft constitute a product different from that which gave rise to the strict liability doctrine on behalf of the general public. Showing a rare understanding of the aircraft acquisition process, the court found for the defendant, Rockwell, relying heavily on the Government's control over specifications and adherence thereto. It also cited the fact that military personnel accept risks different from others, and the concomitant financial protection provided by the Government for its employees and/or their families takes them out of the general public category for which strict liability was created. The court felt a cause of action in negligence was available if the facts so warranted, but strict liability was ruled out as a matter of law. Whether this holds up during what most surely will be a case taken to the Supreme Court remains to be seen. The Circuit Court's decision was not unanimous and a rehearing is already scheduled.

Actually, this case might have more startling ramifications for system safety than for liability. If a manufacturer can diminish his exposure to strict liability by careful identification and reasonable control of hazards with Government cooperation and approval, he will choose that path. That approach is exactly what system safety is all about.

McKay also raised the question of how much the Government knew about the alleged defect, suggesting that as long as the hazard identification and control processes were, in effect, a joint operation, perhaps even the Government might be liable if it were not for the discretionary exclusion under the Federal Tort Claims Act. The key point is whether or not the Government employee is performing a function that could just as well be done by a non-Government employee, and the degree of specificity of the procedures he or she is following. Thus, Government use of one contractor to monitor another contractor's system safety efforts comes into question as do the system safety procedures being imposed.

In handling these litigation-induced safety communication problems, the Departments have carefully modified their investigative and mishap prevention regulations/manuals to assure that the handling of mishap reports does not destroy their privilege status (protection against disclosure). Careful distinction is made between safety and other forms of investigations with only safety enjoying privileged status. Distribution and review of reports are limited to safety personnel within the Government (with occasional exceptions).

Bills have been introduced in Congress to give statutory protection to the mishap report privilege which, to date, has depended upon case law for support. The most recent attempt was tied to the 1984 Defense Authorization Bill; however, once again, the proposal failed to receive Congressional approval.

The Government and contractors have thus far just lived with lawyers' requests for data other than mishap reports. At present, most of the aviation bar does not really understand how to ask the questions beyond asking occasionally for hazard analyses. Once they do, system safety data may well need some protection similar to mishap reports. That this can be done under existing laws is open to considerable doubt.

In terms of OSD policy implications, the situation is potentially critical to the future of system safety programs. It is only a matter of time until the legal profession finds the value (to them) of the full range of system safety documentation and tries to exploit corporate or Government hazard identification and control efforts to their clients' benefit. Current trends in the law should be studied and steps taken accordingly to avoid the inevitable conflict between this eventuality and effective system safety efforts.

## 8. RECOMMENDATIONS

The following recommendations identify management initiatives that would improve the effectiveness of system safety in aircraft acquisition programs. Since the scope of the study included all of OSD and the Military Departments, some of the recommendations are identified with organizations other than OASD(MRA&L). Such recommendations are not being made directly to the associated organization but rather to ASD(MRA&L) to take whatever action he deems appropriate. The recommendations are grouped according to the intended implementing organization or activity: OSD, each Military Department and the JSSC/SSP.

### OFFICE OF THE SECRETARY OF DEFENSE

The recommendations for OSD are presented in six categories: top management support, organization and staffing, policy, legislative initiatives, contracting, and management information.

#### Top Management Support

The Deputy Secretary of Defense should issue to the Secretaries of the Military Departments a sequel to the Deputy Secretary of Defense's (Carlucci) 1981 memorandum on aviation safety [35]. It should include:

1. a clear statement of support for system safety, encompassing the definition of system safety and its relationship to the other safeties. It should also cite the FY84 Defense Guidance requirement to strengthen system safety.
2. A mandate to develop and procure crash-survivable FDRs for all new production aircraft (including the B-1B and F/A-18) and, if possible, retrofit of existing front-line combat aircraft.
3. A request for the Departments to report on the aviation safety initiatives described in their January 1982 responses to the Carlucci memorandum, including a general review and assessment of initiatives to strengthen system safety. Suitable specific

items to be included in the review are identified below under "Management Information."

#### Organization and Staffing

1. The ASD(MRA&L) should establish a position for an experienced system safety professional in the Office of Safety and Occupational Health Policy; such an individual would have duties and responsibilities approximating those described in Appendix A. In order to be effective, this position should be at the GS-15 or military equivalent level.
2. The USDRE should establish a position for an experienced system safety professional in the Office of the Director, Defense Test and Evaluation, with duties and responsibilities approximating those described in Appendix B. This position should also be at the GS-15 level. DoDD 5000.3 ("Test and Evaluations") should be reviewed and revised as necessary in order to reflect the new role of system safety in Defense Test and Evaluation.
3. The ASD(MRA&L) should consider establishing the current Office of Safety and Occupational Health Policy at a higher organizational level, either reporting directly to the ASD or to the Principal DASD. (If such a move is organizationally impractical, then the office should remain where it is, since there is no compelling reason to place the activity under any of the other DASDs in OASD(MRA&L).)
4. The ASD(MRA&L) should, in cooperation with the USDRE, establish a System Safety Review Board (or some equivalent title) to give high-level visibility to broad issues of system safety. This body would address matters such as policy, personnel, improved measures of system safety effectiveness, and assessment of long-term trends. It would maintain a close relationship with the JSSC/SSP. Representation would include OSD and top-level system safety representatives in the Military departments.

#### Policy

1. The Deputy Secretary of Defense should revise DoDD 1000.3 ("Safety and Occupational Health Policy for the Department of Defense") to include a reference to "system safety" in paragraph B ("Applicability and Scope"). Further, amend paragraph D.1.h. to refer to "system safety engineering and management principles" in place of "system safety engineering principles." These changes will help ensure that system safety is accorded appropriate recognition and scope in the top-level DoD policy statement on safety and occupational health.
2. The Deputy Secretary of Defense should revise DoDI 5000.2 ("Major Systems Acquisition Procedures") to give better visibility to system safety. The current format for the

Integrated Program Summary (Enclosure 5 to DoDI 5000.2) does not require safety to be addressed. Rather, safety is to be treated "as required," i.e., if comments to the draft Integrated Program Summary indicate the need. We recommend that safety be automatically included in the Integrated Program Summary; otherwise, there may be nothing to comment on at the OSD level. We also recommend that the treatment of safety, as described in the current Integrated Program Summary format, be modified to require a pre-DSARC briefing of all identified significant hazards, including their resolution and the acceptance of risk. Further, we recommend that the DCP format be modified to include, in the data displays (Annex C and/or Annex D), a separate line-item for "attrition" aircraft, including the associated cost. That is, the increase in the production quantity of aircraft due to expected losses from mishaps should be made visible.

3. The ASD(MRA&L) should make several changes to the top-level policy directive on system safety, DoDI 5000.36 ("System Safety Engineering and Management")<sup>1</sup>:
  - a. Revise to reflect the (herein proposed) system safety responsibilities assigned to OUSDRE/Defense Test and Evaluation.
  - b. Revise for consistency with the above-recommended changes to DoDI 5000.2. Specifically, changes will be required to paragraph E.1.b. ("Responsibilities of the ASD(MRA&L)) and paragraph E.2. ("Responsibilities of the Heads of DoD Components"). We recommend that the exact wording of the changes be done in coordination with the current efforts of the JSSC/SSP to strengthen DoDI 5000.36.
  - c. Paragraph E.1.a. should be revised to read "monitor the application of system safety programs in the DoD acquisition process and throughout the life cycle of systems." (Underlining denotes added words.)
  - d. Add to section E.2. a requirement to ensure assignment of an integrating contractor or Government activity for the integration of hazard information pertaining to GFE.
  - e. Add to section E.2. a requirement to ensure that safety benefits available via new technologies are actively pursued, especially to include hardware systems which do not necessarily contribute to the performance of the aircraft but have payoff in terms of reduced losses via improved accident prevention. Examples of such systems include FDRs, GPWSs, and collision avoidance systems.
  - f. Add to paragraph E.2.a.(a) the phrase "...and that opportunities to enhance system safety based on operational experience are actively sought and acted upon."

---

<sup>1</sup>A copy of this directive is provided in Appendix C.

- g. Add to section E.2. the responsibility to ensure that system safety and human-factors engineering activities are properly coordinated, including the exchange of analyses and reports, and cross-participation in appropriate meetings (such as System Safety Working Group meetings).
4. The ASD(MRA&L) should revise DoDI 6055.7 ("Mishap Investigation, Reporting and Recordkeeping") to broaden the scope of the annual MBO review of safety and occupational health programs to include system safety. At present, the MBO reviews are almost exclusively oriented to matters other than system safety. These reviews are the only existing formal mechanism for the ASD(MRA&L) to monitor the broad application of system safety programs (opportunities to review selected individual major programs occur via the DSARC process) pursuant to his principal responsibilities defined in DoDI 5000.36. Candidate items to be included in the system safety reviews are identified below under "Management Information." Consideration also should be given to incorporating the MBO review requirements of the instruction into a separate instruction under a title such as "Safety Management Information Requirements." The basic orientation of DoDI 6055.7 is mishap reporting and, as such, may not be broad enough to properly accommodate the suggested scope of the MBO reviews.

#### Legal Considerations

1. The ASD(MRA&L) should, with the assistance of the Office of General Counsel (OGC), closely monitor developments in litigation affecting system safety. Further, the OGC might consider preparation of an amicus curiae brief supporting of the recent 9th Circuit Court of Appeals' decision in McKay v. Rockwell, which limited the aircraft manufacturer's exposure to strict liability. (Note: the significance of this decision is that it could provide a strong incentive for contractors to implement aggressive system safety programs -- i.e., the contractor would be exempt from strict liability if, assuming certain other conditions are obtained, he previously identified an accident-producing hazard and warned the Government of same.)

#### Contracting

1. The ASD(MRA&L) should promote the use of award fee criteria for contractor performance of system safety tasks in aircraft acquisition programs. OSD system safety representatives, working with the Defense Acquisition Executive and the System Safety Panel of JSSC, should seek new aircraft programs for the application of such contracting incentives.
2. ASD(MRA&L) should, via the JSSC/SSP, also encourage the tailoring of MIL-STD-881A to identify system safety tasks in the work breakdown structure of aircraft acquisition contracts. This will help ensure the funding and tracking of contractor system safety efforts.

### Management Information

1. The annual MBO review of safety and occupational health should address system safety activities to include items such as the following (to be supported by a written report):
  - a. manpower issues (viz., availability and assignment of qualified personnel in sufficient quantity);
  - b. contracting practices to ensure the performance of necessary system safety tasks, including the use of contract incentives and tailoring of the work breakdown structure (MIL-STD-881A) to include system safety tasks;
  - c. funding for system safety programs, both Government (internal) and contractor efforts in support of major system acquisitions;
  - d. use of independent safety reviews, especially in the acquisition of major systems;
  - e. manner of addressing system hazards in SARCs as required by DoDI 5000.36;
  - f. cost of modification programs to correct hazards/safety deficiencies;
  - g. identification of opportunities for the reduction of aircraft mishap rates and safety modification costs;
  - h. initiatives to take advantage of safety enhancements available via new technology;
  - i. status of efforts to reduce human error accidents (including those which are design-related);
  - j. interface and coordination of system safety and human factor engineering activities;
  - k. organizational and management practices to provide sufficient visibility for system safety and to promote management interest among contractors;
  - l. description of how system safety effectiveness is assured in all phases of the life cycle of systems;
  - m. documentation of major achievements in system safety; in particular, citation of notable "saves" (i.e., accidents or probable accidents avoided) via system safety programs;
  - n. overview of "lessons learned" relative to the strengthening of system safety programs.

2. ASD(MRA&L) should conduct a survey of the DoD Components to determine, for each major mishap category (e.g., Government motor vehicles, injuries and occupational illness, flight mishaps, and private motor vehicles) the annual investment levels (including numbers of personnel) in preventive measures and the associated dollar losses being incurred. Further, the requested data should include a breakout of investment in aircraft system safety separate from the total investment in aviation safety. The results should provide some insights into whether or not safety and occupational health program investments are roughly in balance with the need in each area of safety activity. More specifically, it may allow some judgments to be made about the reasonableness of the investments being made in aircraft system safety programs vis-à-vis the investments in other areas of safety and occupational health. The request to the Departments for these data could probably be accommodated as part of the MBO review process.
3. The ASD(MRA&L) and the USDRE should continue to sponsor periodic safety-technology meetings. The productivity of these meetings might be increased by broadening the participation to include representatives from industry and by narrowing the range of subjects to specific areas of safety and technology.

#### U.S. ARMY

1. The Army's OTEA should be actively involved in system safety. Accordingly, revisions may be required to AR 385-16. OTEA should include system safety professionals who participate in system safety activities throughout the acquisition cycle. The assistance of the ASC should be utilized in defining and organizing an appropriate system safety activity within OTEA.
2. The ASC and the DARCOM Safety Office should jointly develop a program to (1) increase the participation of system safety in early (advanced technology) research and development programs, (2) assure adequate system safety review of system modifications, (3) improve the integration of human factors engineering with system safety efforts, and (4) assure life cycle integration of system safety activities.
3. The top Army regulation on safety, AR 385-10 ("The Army Safety Program"), should be modified to give recognition to system safety. At a minimum, it should be referenced in the sections on "Policy" and "Responsibilities" (especially under the responsibilities of the Deputy Chief of Staff for Personnel and the Commander of DARCOM).
4. DARCOM should consider reestablishing its master's program as an incentive for recruiting and retaining professional system safety personnel.

## U.S. NAVY

1. CNO should strengthen the role of the CNO Safety and Occupational Health Coordinator (OP-09F). This office should be given an activist role in order to project a top-level Navy interest in system safety. The office should be visibly involved in broad areas such as:
  - a. Ensuring the implementation of Navy directives on system safety; in particular, implementation of the CNO responsibilities for system safety under the recently issued SECNAVINST 5100.10E (14 February 1983), which includes the requirement for independent safety assessments in the acquisition cycle of major systems.
  - b. Assessing and supporting periodically the need for funding commensurate with responsibilities assigned to Navy system safety offices, in effect, acting as an ombudsman for system safety.
  - c. Maintaining liaison with system safety offices throughout the Navy in order to be informed about major issues and activities affecting the implementation of system safety programs.
  - d. Coordinating all the safeties (e.g., aviation, occupational safety and health, explosives, nuclear, etc.).
  - e. Promoting communication and coordination between system safety and other activities, such as advanced technology and human factors engineering.
  - f. Promoting the identification and adoption of management initiatives to strengthen system safety effectiveness, such as improved methods of contracting for system safety.
  - g. Assessing system safety manpower needs and developing coordinated recommendations relative to corrective actions.
  - h. Supporting inter-service activities (viz. JSSC), government-industry organizations and professional society activities.

One way to accomplish this would be to establish system safety as a "Specified Support Area" under the provisions of OPNAVINST 5100.8F with responsibility therefore assigned to OP-09F. System Safety certainly meets the "special attention and/or technical expertise" criterion set forth in paragraph 5(b)(2) of the instruction. This alternative could accommodate all the functions indicated above but, more importantly, would integrate and coordinate the Navy's diverse safety activities, including the allocation of resources for safety.

2. In order to adopt the role described above, the OP-09F office should have at least one full-time, experienced system safety professional in addition to the current single O-6 level position.

3. The CNO should increase the impact of the NSC in system safety. There is currently only one experienced system safety professional at the NSC. Additional staff and funding should be authorized in order to establish this office in an effective role in the Navy. Working in conjunction with the OP-09F office, the NSC should exert a strong influence in the practice of system safety throughout the Navy. It should be active in a wide variety of activities, including:
  - a. assessing safety implications of developments in new technology and promoting the adoption of safety-enhancing technology when appropriate;
  - b. providing an independent view of system safety programs throughout the Navy, including participation in System Safety Working Groups and input to the Navy System Acquisition Review Councils;
  - c. revising mishap investigation procedures to incorporate the identification of deficiencies in system safety programs;
  - d. improving the life cycle impact of system safety, in particular the practice of system safety in the NARFs and in the operating commands;
  - e. working with OP-09F in the identification of needed policy development;
  - f. improving the safety "lessons learned" data base and its utilization, especially in the early stages of new programs;
  - g. supporting interservice, industry, and professional society activities;
  - h. supporting special studies as required.
4. The title of OPNAVINST 3750.6N, "Naval Aviation Safety Program," is somewhat misleading and should be changed to more accurately reflect its narrower scope, which is mishap investigation and operational safety. An alternative would be to describe the total aviation safety program in one document and accident investigation and reporting in another.
5. The Chief of Naval Material should review the organization and staffing of its safety office (NMAT-00F) relative to the responsibilities set forth in NAVMATINST 5100.6A. The referenced directive is well written and the requirements therein fully justifiable. Our conclusion, however, is that, with other occupational safety and health matters demanding full attention, the one individual currently in the NMAT-00F office cannot begin to discharge the responsibilities, both stated and implied, in the directive. For the sake of comparison, it is noted that the corresponding offices in the development commands of the Air Force (AFSC) and the Army (DARCOM) have, respectively, four and three full-time professionals devoted purely to system safety activities.

6. The responsibilities of the safety office (AIR-516C) in the Engineering Support and Product Integrity Management Division under the Assistant Commander for Systems and Engineering (AIR-05) should be stated in NAVAIRINST 5100.3B. Further, the role of this office, relative to the following other NAVAIR activities and offices should be better defined:
  - a. The PMA;
  - b. The "Designated Principal for Safety," required by NAVMATINST 5100.10;
  - c. "Class Desk";
  - d. Naval Air Engineering Center;
  - e. NAVAIR Field Stations.
7. The staffing and funding for system safety in NAVAIR should be reviewed relative to the responsibilities assigned in NAV-AIRINST 5100.3B. Justification for this recommendation is based on the following observations:
  - a. The AIR-516C office, which has system safety cognizance over dozens of major programs, currently has one full-time system safety professional plus the services of one contracted individual.
  - b. Working-level system safety engineering support to individual programs is provided by NAEC, located at Lakehurst, New Jersey. The group at NAEC has recently increased from 4 to 10 individuals, none of whom is experienced in system safety.
  - c. The terms of agreement by which NAEC resources are committed to the support of NAVAIR system safety programs are not clear and should be clarified.
  - d. There is no CNO-level sponsor for system safety activities during the budget cycle.
  - e. Although a detailed evaluation of contractor system safety efforts was not made in this study, our observation is that such efforts are spotty and probably underfunded. (The contractor's system safety effort on the F-18 program, for example, is currently operating somewhere around a one-half- to two-person level of effort. We believe that such an effort is prima facie inadequate in the face of the high cost of this complex weapon system. For the sake of comparison: (1) The Army's Advanced Attack Helicopter (AH-64) program supports a four- to five-person level of effort for system safety; (2) the Air Force's B-1B program supports about six system safety professionals in the program director's office (SPO) and over 30 contractor personnel; (3) NASA's Space Shuttle program supports over 20 prime contractor system safety specialists, about 45 NASA specialists at

Johnson Space Center, plus a support contractor at Johnson Space Center.)

8. The Naval Aviation Executive Institute should include a session on system safety in its training program.
9. Although this study restricted its scope to aircraft acquisition programs, it became apparent that there is widespread feeling among the Navy's system safety personnel that the practice of system safety has serious deficiencies in the acquisition and operation of other classes of systems, such as missiles and surface ships. It is, therefore, suggested that this matter be reviewed.

#### U.S. AIR FORCE

1. A program to develop and install a crash-survivable FDR for the B-1B should be initiated immediately.
2. The RCM program, as described in AFLC/AFSC Regulation 66-35 ("Scheduled Maintenance Program"), should be reviewed and modified as necessary to define the relationship of RCM analyses to system safety hazard analyses. Since the RCM analysis (which is the heart of the RCM program) is usually preceded by both system safety and reliability analyses, it is important that the RCM analysis take account of the earlier analyses, particularly those which identify safety critical items.
3. Improve the coordination between system safety and human factors engineering activities. Products of human factors engineering (e.g., analyses of human error and deficiency reports generated during test and evaluation) should be input to the system safety program, and vice versa; results of system safety studies (e.g., hazard analyses and "lessons learned") should be input to the human factors activity. Human factors engineering should be represented at SSG meetings. More generally, the role of human factors engineering in the acquisition process should be reviewed with respect to improving its effectiveness.

#### JOINT SERVICES SAFETY CONFERENCE/SYSTEM SAFETY PANEL

We recommend that the JSSC/SSP consider the following agenda items:

1. JSSC/SSP should address the issue of cost of safety modifications, including (1) the definition of safety modifications, (2) the authority for assigning "safety" as the reason for proposed modifications, and (3) the basis for costing (e.g., ECP-quoted costs or negotiated costs, and the costs of modification installation). A uniform way of collecting and reporting such costs would be desirable. (See OSD Recommendation: "Management Information" f.)
2. JSSC/SSP should promote the use of safety information feedback loops; that is, the feedback of safety performance information from the field (both T&E and operational use) to the system safety program. The USAF "Feedback Policy" (AFR 800-13) is an example of such a feedback system.

3. The accident investigation and analysis process should be broadened to include, where feasible, the identification of causal factors which can be attributed to deficiencies in the associated system safety program. The safety centers are the most logical activity to perform this function due to their relatively independent status. Such an effort should produce useful "lessons learned" pertaining to the management and implementation of system safety efforts.
4. Establishment of an all-Service incident reporting program analogous to the FAA/NASA Aviation Safety Reporting System to improve the understanding of human error, obtained directly from the operating personnel involved in the incidents.
5. Software system safety should be a matter for continuing JSSC/SSP attention and is an ideal topic for interservice/industry cooperative efforts. Consideration should be given to establishing a JSSC/SSP subcommittee patterned after the current Air Force Software Systems Safety Committee, to include representatives from industry and academia. Recognition must be given to the interdisciplinary nature of the software system safety problem and, thus, the need for communication and coordination with other disciplines.
6. A renewed and determined effort should be made, in cooperation with OSD(MRA&L), to find an acceptable solution to the problem of an inadequate job classification for system safety professionals.
7. Closely follow and attempt to adapt, as appropriate, the experience of the Air Force AFSC/Space Division with award fee contracting for the performance of safety tasks. Consider preparation of a guidelines document, to be used by government officials and contractors, for system safety award fee contracting. Promote interservice crossfeed relative to techniques for improved system safety contracting.
8. JSSC, in cooperation with OSD, should promote a system safety/human factor engineering dialogue in order to better define the interface of the two disciplines. At a minimum, such communications should occur between the System Safety and Life Sciences panels of the JSSC. Meetings in a wider forum should also be considered, perhaps in cooperation with groups such as the DoD Technical Advisory Group on Human Factors, the Electronic Industries Association's G-48 Committee, and individuals from human factors engineering activities in the military departments and industry.
9. Both MIL-STD-882A (System Safety) and MIL-STD-46955 (Human Factors Engineering) should be modified to incorporate a requirement for coordination and integration of each discipline with the other.

## APPENDIX A

### GENERAL DUTIES AND RESPONSIBILITIES FOR SYSTEM SAFETY SPECIALIST IN OASD(MRA&L)

- Promote system safety within the DoD.
- Project strong OSD image to the Services, the professional community, and industry.
- Maintain close liaison with counterparts in Services in order to understand policy developments and issues relative to system safety.
- Identify general policy needs and work to accomplish necessary changes.
- Emphasis on broad issues, such as:
  - changes to MIL-STD-882, DoDI 5000.36, and DoDI 5000.2;
  - communication to top DoD management of system safety needs and accomplishments;
  - promotion of better interface between system safety, human factors, and other disciplines;
  - development of innovative approaches to incentivize system safety performance by contractors;
  - improving the application and integration of system safety efforts throughout life cycle;
  - development of information systems (e.g., "lessons learned");
  - find feasible solutions to personnel-related issues.
- Work closely with counterparts in OUSDRE to assure effective OSD participation in DSARC process and in identification of research needs.
- Assure effective OSD role in MBO reviews relative to system safety.

## **APPENDIX B**

### **GENERAL DUTIES AND RESPONSIBILITIES FOR SYSTEM SAFETY SPECIALIST IN OUSDRE/TEST AND EVALUATION**

- Monitor and promote the inclusion of effective system safety programs during the acquisition phase of all major system procurements by the Services.
  - Establish liaison with system safety principals on major acquisition programs for the specific purpose of maintaining an awareness of the acceptance of risk.
  - Review and comment on Test and Evaluation Master Plans and on test results.
  - Provide safety-pertinent inputs to the Director Defense Test and Evaluation for DSARC reviews.
  - Participate in pre-DSARC safety briefings. Review the "for comment" DCPs and provide inputs to the system safety representative in MRA&L.
- Work closely with counterparts in OASD(MRA&L) to identify needs and sponsor system safety research programs.

APPENDIX C



December 6, 1978  
NUMBER 5000.36

---

---

## Department of Defense Instruction <sup>ASD(MRA&L)</sup>

**SUBJECT**            System Safety Engineering and Management

- References:**
- (a) DoD Directive 1000.3, "Accident Prevention Safety and Occupational Health Policy for the Department of Defense," June 15, 1976
  - (b) DoD Directive 5000.1, "Major System Acquisitions," January 18, 1977
  - (c) DoD Directive 5000.2, "Major System Acquisition Process," January 18, 1977
  - (d) through (h) see enclosure 1

### **A. PURPOSE**

The purpose of this Instruction is to reduce the number and severity of DoD mishaps through the organized use of system safety engineering and system safety management. This Instruction amplifies the system safety policy set forth in reference (a), and is especially pertinent to the system acquisition process established in references (b) and (c).

### **B. APPLICABILITY AND SCOPE**

1. The provisions of this Instruction apply to the Office of the Secretary of Defense, the Military Departments, the Organization of the Joint Chiefs of Staff, the Defense Agencies and the Unified and Specified Commands (hereafter referred to as "DoD Components").
2. This Instruction is not intended to modify the safety requirements for chemical and nuclear systems as prescribed in DoD Instruction 4120.13 (reference (d)) and DoD Directive 5030.15 (reference (e)).

### **C. DEFINITIONS**

Terms as used in this Instruction are defined in enclosure 2.

### **D. POLICY**

1. System safety engineering and management programs shall be used in accordance with criteria and procedures set forth herein to ensure that the highest possible degree of safety and occupational health, consistent with mission requirements and cost effectiveness, is designed into DoD systems and facilities. These system safety programs shall commence with program initiation and continue through the life cycle of the program.

4. Primary emphasis will be placed on the identification, evaluation, and elimination or control of hazards prior to the production and deployment phase of systems or the construction phase of facilities.

3. These programs shall be in consonance with the uniform requirements to develop and implement tailored system safety programs as prescribed in Military Standard 882A (reference (f)).

#### **E. RESPONSIBILITIES**

1. The Assistant Secretary of Defense (Manpower, Reserve Affairs, and Logistics) shall:

a. Monitor the application of system safety programs in the DoD acquisition process.

b. Review the "for comment" decision coordinating papers to ensure that safety risks have been addressed according to the requirements set forth in paragraph 2.b. below.

c. In coordination with the Under Secretary of Defense for Research and Engineering, establish and support system safety engineering research projects.

2. The Heads of DoD Components shall:

a. Establish system safety programs and apply Military Standard 882A (reference (f)), tailored in accordance with DoD Directive 4120.21 (reference (g)), for each major system acquisition. Military Standard 882A shall also be applied in the acquisition of other systems and facilities, as appropriate, based upon the severity of associated hazards and the potential for loss or damage of DoD resources. These system safety programs shall:

(1) Provide for an initial assessment of safety risks at program initiation to define the scope and detail of system safety program requirements.

(2) Integrate system safety engineering and management into the total system acquisition program so that system safety program milestones are consistent with other engineering and program management milestones.

(3) Ensure that historical safety data (lessons learned) from previous system acquisitions are considered and used where appropriate.

(4) Eliminate or control:

(a) System hazards prior to the production and deployment phase.

(b) Facility hazards prior to the construction phase.

(5) Use risk assessment and life cycle cost analyses to determine priorities to correct identified hazards.

(6) Establish procedures to ensure timely follow-up on identified hazards and to implement corrective action.

(7) Establish formal documentation of each management decision, if any, to accept the risks associated with an identified hazard.

(8) Ensure that system safety is considered in all testing. Where normal testing is insufficient to demonstrate safe operation, prepare and monitor special safety tests and evaluations.

(9) Require a follow-on system safety effort to ensure that changes made after deployment do not introduce hazards or degrade existing levels of system safety.

(10) Develop procedures for the safe and environmentally acceptable disposal or demilitarization of any hazardous materials associated with the system.

(11) Plan for the development of data required to identify hazardous materials and items as prescribed in DoD Instruction 6050.5 (reference (h)).

b. Provide for system safety hazard assessments at design and program reviews. For major system acquisitions, furnish these assessments to the Service Acquisition Review Councils. Moreover, inform the Assistant Secretary of Defense (Manpower, Reserve Affairs, and Logistics) of any significant hazards relative to major systems prior to the Milestone II decision.

c. Apply the requirements specified here to off-the-shelf procurement items with potential for critical or catastrophic failures; and to DoD "in-house" development, production, modification and test programs.

Dec 6, 78  
5000.36

**F. EFFECTIVE DATE AND IMPLEMENTATION**

This Instruction is effective immediately. Forward one copy of each implementing document to the Assistant Secretary of Defense (Manpower, Reserve Affairs and Logistics) within 120 days.



**ROBERT B. PIRIE, JR.**  
Acting Assistant Secretary of Defense  
(Manpower, Reserve Affairs, and Logistics)

Enclosures - 2

1. References
2. Definitions

5000.36 (Encl 1)  
Dec 6, 78

REFERENCES, continued

- (d) DoD Instruction 4120.13, "Safety Program for Chemical Agents and Associated Weapon Systems," April 30, 1970
- (e) DoD Directive 5030.15, "Safety Studies and Reviews of Nuclear Weapons Systems," August 8, 1974
- (f) Military Standard 882A, "System Safety Program Requirements," June 28, 1977
- (g) DoD Directive 4120.21, "Specifications and Standards Application," April 9, 1977
- (h) DoD Instruction 6050.5, "Hazardous Material Information System," January 25, 1978

**DEFINITIONS**

- A. **Mishap.** An unplanned event or series of events that result in death, injury, occupational illness, or damage to or loss of equipment or property.
- B. **Hazard.** An existing or potential condition that can result in a mishap.
- C. **System Safety Engineering.** An element of system engineering requiring specialized professional knowledge and skills in the application of scientific and engineering principles, criteria, and techniques for the timely identification and elimination or control of hazards.
- D. **System Safety Management.** An element of management that ensures the planning, implementation, and accomplishment of tasks and activities to meet identified system safety requirements, consistent with overall program requirements.
- E. **System Safety Program.** The combined tasks and activities of system safety management and system safety engineering that enhance operational effectiveness by satisfying the system safety requirements in a timely, cost-effective manner throughout all phases of a system life cycle.

## APPENDIX D

### REFERENCES

1. General Accounting Office, "Acquiring Weapons Systems in a Period of Rising Expenditures: Implications for Defense Management," NASD-81-26, Washington, General Accounting Office, 14 May 1981.
2. Miller, C. O., "Why System Safety," MIT Technology Review, February 1971.
3. Department of Defense, Office of the Deputy Secretary of Defense (Frank Carlucci), "Memorandum, Subject: Aviation Safety," September 18, 1981.
4. Department of Defense, Assistant Secretary of Defense (Manpower, Reserve Affairs and Logistics), Department of Defense Directive 5124.1, Washington, Department of Defense, April 20, 1977.
5. Department of Defense, "Mishap Investigation, Reporting and Record-keeping," Department of Defense Instruction 6055.7, Washington, Department of Defense, December 16, 1981.
6. Wade, James P., "Aviation Systems Safety," Memorandum for the Assistant Secretary of Defense (Manpower, Reserve Affairs and Logistics), 24 May 1982.
7. Department of Defense, "Test and Evaluation," Department of Defense Directive 5000.3, Washington, Department of Defense, December 26, 1979.
8. Weinberger, C. W., "Occupational Safety and Health," A Memorandum for Secretaries of the Military Departments, Directors of Defense Agencies, 7 January 1983.
9. Department of Defense, Software Technology for Adaptable, Reliable Systems (STARS), Volumes: "Joint Task Force Report," "Program Strategy," and "Implementation Approach," Washington, Department of Defense, Circa Winter 82-83.
10. U.S. Navy, "Navy System Safety Coordination Meeting Minutes of 19 January 1982," Naval Safety Center, Forward by a letter from C. R. Compton, 3 February 1982.
11. Miller, C. O., "Why System Safety," MIT Technology Review, February 1971.
12. U.S. Air Force AFLC/AFSC, "Joint AFLC/AFSC Lessons Learned Program," AFLC/AFSC Reg. 800.37, Washington, U.S. Air Force, 7 August 1981.
13. U.S. Air Force, AFLC, "AFALD Lessons Learned Program," AFLC HQ Operating Instruction 800-1, Washington, U.S. Air Force, 15 December 1982.
14. Hicks, Chauncey, "1983 Worldwide Safety Conference," USAF Safety Journal, May 1983.

15. Stewart, Colonel Sam P., "Minutes of the First AFSC Commanders System Safety Policy Group Meeting," 21 December 1982.
16. United States Air Force, Safety Journal, Washington, U.S. Air Force, May 1983.
17. Mitchell, Major General John H., Remarks before the 1982 JSSC, Fort Rucker, Alabama, 29 September 1982.
18. U.S. Navy, "General Specification for Design and Construction of Aircraft Weapon Systems," Volume I, SD-24L, Washington, U.S. Navy, 2 June 1982.
19. Steele, Rear Admiral T.C., "Aircraft Mishap Analysis Point Paper," Naval Safety Center, (Forwarded to Director of Safety and Occupational Health, Office of the Secretary of Defense, 27 May 1983).
20. Briefing Charts on "U.S. Navy Ground Proximity Warning System," Doc No. 82-P926C, Unclassified.
21. Miller, C. O., "Recent Trends in Human Factors Analysis in Aviation Accidents," System Safety Inc., Presented at the 6th Annual Aviation Law Seminar sponsored by the Florida Bar Association, Tampa, Florida, November 5, 1982.
22. Department of Defense, "Human Engineering Requirements for Military Systems, Equipment and Facilities," MIL-H-46855B, Washington, Department of Defense, 31 January 1979.
23. Fineberg, Michael, et al., "Definition of Investigative Areas for Human-Factor Aspects of Aircraft Accidents," SAM-TR-80-48, BDM Corporation, McLean, Virginia Prepared for USAF School of Aerospace Medicine, December 1980.
24. National Research Council, "An Evaluation of NASA's Program in Human Factors Research," National Academy Press, 1982.
25. Zeller, A. F., "Three Decades of USAF Efforts to Reduce Human Error Accidents (1947-1977)," November 1978.
26. Defense Audit Service, "Report on the Review of Air Crew Safety Programs," Report Number 81-025, December 8, 1980.
27. Government Accounting Office, "Guidelines for Assessing Whether Human Factors Were Considered in the Weapon Systems Acquisition Process," Washington, General Accounting Office, 8 December 1981.
28. U.S. Army, "Aircraft Accident Prevention, Investigation and Reporting," AR 95-5, Washington, U.S. Army, 1 July 1975.
29. U.S. Army, "Human Factors Engineering Program," AR 602-1, Washington, U.S. Army, 15 February 1983.
30. Rimson, I. J., "The Impact of Fly-By-Wire (and Other Computer-Controlled Systems) on Aircraft Accident Investigations".

31. Stencel Aero. Engineering Corp. v. United States, 431 U.S. 666 (1977).
32. Boeing Airplane Company v. Brown, 291 F. 2d 274 (9th Cir., 1961).
33. McKay v. Rockwell International Corp., 704 F. 2d 444 (9th Circuit, 1983).
34. Department of Defense, Office of the Deputy Secretary of Defense (Frank Carlucci), "Memorandum, Subject: Aviation Safety," September 18, 1981.

# APPENDIX E

## GLOSSARY OF TERMS

AFFTC	Air Force Flight Test Center
AFISC	Air Force Inspection and Safety Center
AFLC	Air Force Logistics Command
AFPRO	Air Force Plant Representative Office
AFR	Air Force Regulation
AFSC	Air Force Systems Command
AIRS	Accident Information Retrieval System
AR	Army Regulation
ASARC	Army System Acquisition Review Council
ASC	Army Safety Center
ASD(MRA&L)	Assistant Secretary of Defense (Manpower, Reserve Affairs and Logistics)
ASNS&L	Assistant Secretary of the Navy (Shipbuilding and Logistics)
AVRADCOM	Army Aviation Research and Development Command
AVSYCOM	Aviation Systems Command
B-1B	B1 Bomber
CNO	Chief of Naval Operations
CPI	Crash Position Indicator
CPL	Crash Position Locator
DARCOM	Department of Army Materiel Development and Readiness Command
DAS	Directorate of Aerospace Safety
DCNM	Deputy Chief of Naval Material
DCP	Decision Coordinating Paper
DCS	Deputy Chief of Staff
DCSPER	Deputy Chief of Staff for Personnel
DMSSO	Defense Materiel Specifications and Standards Office
DNSARC	Department of the Navy Systems Acquisition Review Council
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction

DSARC	Defense Systems Acquisition Review Council
ECP	Engineering Change Proposal
EOSP	Equal Opportunity and Safety Policy
FAA	Federal Aviation Administration
FDR	Flight Data Recorder
FMEA	Failure Modes and Effects Analysis
FORSCOM	Forces Command
GFE	Government-furnished Equipment
GPWS	Ground Proximity Warning System
HOMR	Human Oriented Mishap Reduction
IG	Inspector General
JSSC	Joint Services Safety Conference
JSSC/SSP	Joint Services Safety Conference/System Safety Panel
LASAS	Low Altitude Safety Alert System
MAJCOMS	Major Commands
MBO	Management By Objectives
MENS	Mission Element Needs Statements
MIL-STD	Military Standard
MSRDS	Maintenance Signal Data Recording System
NAEC	Naval Air Engineering Center
NARF	Naval Air Rework Facility
NASA	National Aeronautics and Space Administration
NATC	Naval Air Test Center
NAVAIR	Naval Air Systems Command
NAVAIRSYSCOM	Naval Air Systems Command
NAVMAT	Naval Material Command
NSC	Naval Safety Center
NTSB	National Transportation Safety Board
OASD(MRA&L)	Office of the Assistant Secretary of Defense (Manpower, Reserve Affairs and Logistics)
OGC	Office of General Counsel
OPM	Office of Personnel Management
OPNAV	Office of Chief of Naval Operations
OP-09F	Office of the CNO Safety & Occupational Health Coordinator
OSD	Office of the Secretary of Defense
OSD(MRA&L)	Office of the Secretary of Defense (Manpower, Reserve Affairs and Logistics)

OSH	Occupational Safety and Health
OTEA	Operational Test and Evaluation Agency
OUSDRE	Office of the Undersecretary of Defense Research and Engineering
PPB	Planning, Programming and Budgeting
PMA	Program Manager -- Air
PMRT	Program Management Responsibility Transfer
R&M	Reliability and Maintainability
RCM	Reliability Centered Maintenance
RFP	Request for Proposal
SARC	System Acquisition Review Council
SES	System Safety and Engineering Division
SECNAV	Secretary of the Navy
SOH	Safety and Occupational Health
SOHP	Office of Safety and Occupational Health Policy
SON	Statements of Operational Need
SPO	System Program Office
SSG	System Safety Groups
SSM	System Safety Managers
SSP	System Safety Programs
STARS	Software Technology for Adaptable, Reliable Systems
TEMPS	Test and Evaluation Master Plans
TRADOC	Training and Doctrine Command
TSARCOM	Troop Support and Readiness Command
ULAIDS	Universal Locator Airborne Integrated Data System
USAF	United States Air Force
USDRE	Undersecretary of Defense Research and Engineering
VCNO	Vice Chief of Naval Operations

Unclassified

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER	2. GOVT ACCESSION NO. AD-A141 492	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle)  SYSTEM SAFETY IN AIRCRAFT ACQUISITION		5. TYPE OF REPORT & PERIOD COVERED
		6. PERFORMING ORG. REPORT NUMBER LMI TASK ML214
7. AUTHOR(s)  F. R. Frola C. O. Miller		8. CONTRACT OR GRANT NUMBER(s)  MDA903-81-C-0166
9. PERFORMING ORGANIZATION NAME AND ADDRESS  Logistics Management Institute 4701 Sangamore Road, P.O. Box 9489 Washington, D.C. 20016		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
11. CONTROLLING OFFICE NAME AND ADDRESS  Assistant Secretary of Defense (Manpower, Reserve Affairs and Logistics)		12. REPORT DATE November 1983
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office)		13. NUMBER OF PAGES 127
		15. SECURITY CLASS. (of this report) Unclassified
		15a. DECLASSIFICATION/DOWNGRADING SCHEDULE
16. DISTRIBUTION STATEMENT (of this Report)  "A" Approval for public release; distribution unlimited.		
17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)		
18. SUPPLEMENTARY NOTES		
19. KEY WORDS (Continue on reverse side if necessary and identify by block number)  System safety; aircraft acquisition; management initiatives; policy;		
20. ABSTRACT (Continue on reverse side if necessary and identify by block number)  This report identifies management initiatives for strengthening the effectiveness of system safety in aircraft acquisition programs. More aggressive implementation of existing system safety policy can help reduce the mishap rate and the need for costly modification programs to correct safety deficiencies. Recommendations to OSD and the Military Departments include: (1) the need for continuing top management support; (2) staffing and funding for system safety efforts commensurate with responsibilities set forth in		

Unclassified

SECURITY CLASSIFICATION OF THIS PAGE(When Data Entered)

policy statements; (3) emphasis on the man-machine interface and the associated need for better coordination of system safety and human factors engineering activities; (4) improved methods for detecting system software hazards; (5) better utilization of advanced technology, including flight data recorders, ground proximity warning systems, and collision avoidance systems; (6) writing better contracts with respect to system safety tasks; and (7) more effective recruiting, training, and retention of system safety personnel.

Unclassified

SECURITY CLASSIFICATION OF THIS PAGE(When Data Entered)